MATHEMATICAL REASONING - WRITING AND PROOF

Ted Sundstrom

Grand Valley State University

LibreTexts™

Grand Valley State University

Mathematical Reasoning - Writing and Proof

Ted Sundstrom

This text is disseminated via the Open Education Resource (OER) LibreTexts Project (https://LibreTexts.org) and like the thousands of other texts available within this powerful platform, it is freely available for reading, printing, and "consuming."

The LibreTexts mission is to bring together students, faculty, and scholars in a collaborative effort to provide an accessible, and comprehensive platform that empowers our community to develop, curate, adapt, and adopt openly licensed resources and technologies; through these efforts we can reduce the financial burden born from traditional educational resource costs, ensuring education is more accessible for students and communities worldwide.

Most, but not all, pages in the library have licenses that may allow individuals to make changes, save, and print this book. Carefully consult the applicable license(s) before pursuing such effects. Instructors can adopt existing LibreTexts texts or Remix them to quickly build course-specific resources to meet the needs of their students. Unlike traditional textbooks, LibreTexts' web based origins allow powerful integration of advanced features and new technologies to support learning.

LibreTexts is the adaptable, user-friendly non-profit open education resource platform that educators trust for creating, customizing, and sharing accessible, interactive textbooks, adaptive homework, and ancillary materials. We collaborate with individuals and organizations to champion open education initiatives, support institutional publishing programs, drive curriculum development projects, and more.

The LibreTexts libraries are Powered by NICE CXone Expert and was supported by the Department of Education Open Textbook Pilot Project, the California Education Learning Lab, the UC Davis Office of the Provost, the UC Davis Library, the California State University Affordable Learning Solutions Program, and Merlot. This material is based upon work supported by the National Science Foundation under Grant No. 1246120, 1525057, and 1413739.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation nor the US Department of Education.

Have questions or comments? For information about adoptions or adaptions contact info@LibreTexts.org or visit our main website at https://LibreTexts.org.

The LibreTexts name, logo, and book covers are trademarked by LibreTexts, Inc. (a 501(c)(3) not-for-profit organization) and protected against unauthorized use.

This text was compiled on 07/16/2026

- **InfoPage** by Delmar Larsen is licensed Public Domain.

TABLE OF CONTENTS

Licensing

1: Introduction to Writing Proofs in Mathematics

- 1.1: Statements and Conditional Statements
- 1.2: Constructing Direct Proofs
- 1.S: Introduction to Writing Proofs in Mathematics (Summary)

2: Logical Reasoning

- 2.1: Statements and Logical Operators
- 2.2: Logically Equivalent Statements
- 2.3: Open Sentences and Sets
- 2.4: Quantifiers and Negations
- 2.S: Logical Reasoning (Summary)

3: Constructing and Writing Proofs in Mathematics

- 3.1: Direct Proofs
- 3.2: More Methods of Proof
- 3.3: Proof by Contradiction
- 3.4: Using Cases in Proofs
- 3.5: The Division Algorithm and Congruence
- 3.6: Review of Proof Methods
- 3.S: Constructing and Writing Proofs in Mathematics (Summary)

4: Mathematical Induction

- 4.1: The Principle of Mathematical Induction
- 4.2: Other Forms of Mathematical Induction
- 4.3: Induction and Recursion
- 4.S: Mathematical Induction (Summary)

5: Set Theory

- 5.1: Sets and Operations on Sets
- 5.2: Proving Set Relationships
- 5.3: Properties of Set Operations
- 5.4: Cartesian Products
- 5.5: Indexed Families of Sets
- 5.S: Set Theory (Summary)

6: Functions

- 6.1: Introduction to Functions
- 6.2: More about Functions
- 6.3: Injections, Surjections, and Bijections
- 6.4: Composition of Functions
- 6.5: Inverse Functions
- 6.6: Functions Acting on Sets
- 6.S: Functions (Summary)

7: Equivalence Relations

- 7.1: Relations
- 7.2: Equivalence Relations
- 7.3: Equivalence Classes
- 7.4: Modular Arithmetic
- 7.S: Equivalence Relations (Summary)

8: Topics in Number Theory

- 8.1: The Greatest Common Divisor
- 8.2: Prime Numbers and Prime Factorizations
- 8.3: Linear Diophantine Equations
- 8.S: Topics in Number Theory (Summary)

9: Finite and Infinite Sets

- 9.1: Finite Sets
- 9.2: Countable Sets
- 9.3: Uncountable Sets
- 9.S: Finite and Infinite Sets (Summary)

Index

Appendix A: Guidelines for Writing Mathematical Proofs

Appendix B: Answers for the Progress Checks

Appendix C: Answers and Hints for Selected Exercises

Appendix D: List of Symbols

Detailed Licensing

Licensing

A detailed breakdown of this resource's licensing can be found in ***Back Matter/Detailed Licensing****.*

CHAPTER OVERVIEW

1: Introduction to Writing Proofs in Mathematics

1.1: Statements and Conditional Statements
1.2: Constructing Direct Proofs
1.S: Introduction to Writing Proofs in Mathematics (Summary)

This page titled 1: Introduction to Writing Proofs in Mathematics is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

1.1: Statements and Conditional Statements

Much of our work in mathematics deals with statements. In mathematics, a **statement** is a declarative sentence that is either true or false but not both. A statement is sometimes called a **proposition**. The key is that there must be no ambiguity. To be a statement, a sentence must be true or false, and it cannot be both. So a sentence such as "The sky is beautiful" is not a statement since whether the sentence is true or not is a matter of opinion. A question such as "Is it raining?" is not a statement because it is a question and is not declaring or asserting that something is true.

Some sentences that are mathematical in nature often are not statements because we may not know precisely what a variable represents. For example, the equation $2x+5 = 10$ is not a statement since we do not know what x represents. If we substitute a specific value for x (such as $x = 3$), then the resulting equation, $2\cdot 3 +5 = 10$ is a statement (which is a false statement). Following are some more examples:

✓ Example:

- There exists a real number x such that $2x+5 = 10$.
  This is a statement because either such a real number exists or such a real number does not exist. In this case, this is a true statement since such a real number does exist, namely $x = 2.5$.
- For each real number x, $2x+5=2\left(x+\frac{5}{2}\right)$.
  This is a statement since either the sentence $2x+5=2\left(x+\frac{5}{2}\right)$ is true when any real number is substituted for x (in which case, the statement is true) or there is at least one real number that can be substituted for x and produce a false statement (in which case, the statement is false). In this case, the given statement is true.
- Solve the equation $x^2-7x+10=0$.
  This is not a statement since it is a directive. It does not assert that something is true.
- $(a+b)^2=a^2+b^2$ is not a statement since it is not known what a and b represent. However, the sentence, “There exist real numbers a and b such that $(a+b)^2=a^2+b^2$" is a statement. In fact, this is a true statement since there are such integers. For example, if $a=1$ and $b=0$, then $(a+b)^2=a^2+b^2$.
- Compare the statement in the previous item to the statement, “For all real numbers a and b, $(a+b)^2=a^2+b^2$." This is a false statement since there are values for a and b for which $(a+b)^2\neq a^2+b^2$. For example, if $a=2$ and $b=3$, then $(a+b)^2$ $=5^2=25$ and $a^2+b^2=2^2+3^2=13$.

? Progress Check 1.1: Statements

Which of the following sentences are statements? Do not worry about determining whether a statement is true or false; just determine whether each sentence is a statement or not.

1. $3 + 4 = 8$.
2. $2\cdot 7 + 8 = 22$.
3. $(x-1)=\sqrt{(x+11)}$.
4. $2x+5y=7$.
5. There are integers x and y such that $2x+5y=7$.
6. There are integers x and y such that $23x+27y=52$.
7. Given a line L and a point P not on that line, there is a unique line through P that does not intersect L.
8. $(a+b)^3=a^3+3a^2b+3ab^2+b^3$.
9. $(a+b)^3=a^3+3a^2b+3ab^2+b^3$ for all real numbers a and b.
10. The derivative of $f(x)=\sin x$ is $f'(x)=\cos x$.
11. Does the equation $3x^2-5x-7=0$ have two real number solutions?
12. If ABC is a right triangle with right angle at vertex B, and if D is the midpoint of the hypotenuse, then the line segment connecting vertex B to D is half the length of the hypotenuse.
13. There do not exist three integers x, y, and z such that $x^3+y^2=z^3$.

Answer

Add texts here. Do not delete this text first.

How Do We Decide If a Statement Is True or False?

In mathematics, we often establish that a statement is true by writing a mathematical proof. To establish that a statement is false, we often find a so-called counterexample. (These ideas will be explored later in this chapter.) So mathematicians must be able to discover and construct proofs. In addition, once the discovery has been made, the mathematician must be able to communicate this discovery to others who speak the language of mathematics. We will be dealing with these ideas throughout the text.

For now, we want to focus on what happens before we start a proof. One thing that mathematicians often do is to make a conjecture beforehand as to whether the statement is true or false. This is often done through exploration. The role of exploration in mathematics is often difficult because the goal is not to find a specific answer but simply to investigate. Following are some techniques of exploration that might be helpful.

Techniques of Exploration

- **Guesswork and conjectures**. Formulate and write down questions and conjectures. When we make a guess in mathematics, we usually call it a conjecture.
- **Examples. Constructing appropriate examples is extremely important**. Exploration often requires looking at lots of examples. In this way, we can gather information that provides evidence that a statement is true, or we might find an example that shows the statement is false. This type of example is called a **counterexample**.

✓ Example:

For example, if someone makes the conjecture that $\sin(2x) = 2\sin(x)$, for all real numbers x, we can test this conjecture by substituting specific values for x. One way to do this is to choose values of x for which $\sin(x)$is known. Using $x = \frac{\pi}{4}$, we see that

$$\sin(2(\frac{\pi}{4})) = \sin(\frac{\pi}{2}) = 1, \text{ and}$$

$$2\sin(\frac{\pi}{4}) = 2(\frac{\sqrt{2}}{2}) = \sqrt{2}.$$

Since $1 \neq \sqrt{2}$, these calculations show that this conjecture is false. However, if we do not find a counterexample for a conjecture, we usually cannot claim the conjecture is true. The best we can say is that our examples indicate the conjecture is true. As an example, consider the conjecture that

If x and y are odd integers, then $x + y$ is an even integer.

We can do lots of calculation, such as $3 + 7 = 10$ and $5 + 11 = 16$, and find that every time we add two odd integers, the sum is an even integer. However, it is not possible to test every pair of odd integers, and so we can only say that the conjecture appears to be true. (We will prove that this statement is true in the next section.)

- **Use of prior knowledge.** This also is very important. We cannot start from square one every time we explore a statement. We must make use of our acquired mathematical knowledge. For the conjecture that $\sin(2x) = 2\sin(x)$, for all real numbers x, we might recall that there are trigonometric identities called "double angle identities." We may even remember the correct identity for $\sin(2x)$, but if we do not, we can always look it up. We should recall (or find) that

  for all real numbers x,

$$\sin(2x) = 2\sin(x)\cos(x). \tag{1.1.1}$$

- We could use this identity to argue that the conjecture "for all real numbers x, $\sin(2x) = 2\sin(x)$" is false, but if we do, it is still a good idea to give a specific counterexample as we did before.
- **Cooperation and brainstorming**. Working together is often more fruitful than working alone. When we work with someone else, we can compare notes and articulate our ideas. Thinking out loud is often a useful brainstorming method that helps generate new ideas.

Progress Check 1.2: Explorations

Use the techniques of exploration to investigate each of the following statements. Can you make a conjecture as to whether the statement is true or false? Can you determine whether it is true or false?

1. $(a+b)^2 = a^2 + b^2$, for all real numbers a and b.
2. There are integers x and y such that $2x + 5y = 41$.
3. If x is an even integer, then x^2 is an even integer.
4. If x and y are odd integers, then $x \cdot y$ is an odd integer.

Answer

Add texts here. Do not delete this text first.

Conditional Statements

One of the most frequently used types of statements in mathematics is the so-called conditional statement. Given statements P and Q, a statement of the form "If P then Q" is called a **conditional statement**. It seems reasonable that the truth value (true or false) of the conditional statement "If P then Q" depends on the truth values of P and Q. The statement "If P then Q" means that Q must be true whenever P is true. The statement P is called the **hypothesis** of the conditional statement, and the statement Q is called the **conclusion** of the conditional statement. Since conditional statements are probably the most important type of statement in mathematics, we give a more formal definition.

Definition

A **conditional statement** is a statement that can be written in the form "If P then Q," where P and Q are sentences. For this conditional statement, P is called the **hypothesis** and Q is called the **conclusion**.

Intuitively, "If P then Q" means that Q must be true whenever P is true. Because conditional statements are used so often, a symbolic shorthand notation is used to represent the conditional statement "If P then Q." We will use the notation $P \to Q$ to represent "If P then Q." When P and Q are statements, it seems reasonable that the truth value (true or false) of the conditional statement $P \to Q$ depends on the truth values of P and Q. There are four cases to consider:

- P is true and Q is true.
- P is false and Q is true.
- P is true and Q is false.
- P is false and Q is false.

The conditional statement $P \to Q$ means that Q is true whenever P is true. It says nothing about the truth value of Q when P is false. Using this as a guide, we define the conditional statement $P \to Q$ to be false only when P is true and Q is false, that is, only when the hypothesis is true and the conclusion is false. In all other cases, $P \to Q$ is true. This is summarized in Table **1.1**, which is called a **truth table** for the conditional statement $P \to Q$. (In Table **1.1**, T stands for "true" and F stands for "false.")

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

Table 1.1: Truth Table for $P \to Q$

The important thing to remember is that the conditional statement $P \to Q$ has its own truth value. It is either true or false (and not both). Its truth value depends on the truth values for P and Q, but some find it a bit puzzling that the conditional statement is considered to be true when the hypothesis P is false. We will provide a justification for this through the use of an example.

Example 1.3:

Suppose that I say

“If it is not raining, then Daisy is riding her bike.”

We can represent this conditional statement as $P \to Q$ where P is the statement, “It is not raining” and Q is the statement, “Daisy is riding her bike.”

Although it is not a perfect analogy, think of the statement $P \to Q$ as being false to mean that I lied and think of the statement $P \to Q$ as being true to mean that I did not lie. We will now check the truth value of $P \to Q$ based on the truth values of P and Q.

1. Suppose that both P and Q are true. That is, it is not raining and Daisy is riding her bike. In this case, it seems reasonable to say that I told the truth and that$P \to Q$ is true.
2. Suppose that P is true and Q is false or that it is not raining and Daisy is not riding her bike. It would appear that by making the statement, “If it is not raining, then Daisy is riding her bike,” that I have not told the truth. So in this case, the statement $P \to Q$ is false.
3. Now suppose that P is false and Q is true or that it is raining and Daisy is riding her bike. Did I make a false statement by stating that if it is not raining, then Daisy is riding her bike? The key is that I did not make any statement about what would happen if it was raining, and so I did not tell a lie. So we consider the conditional statement, “If it is not raining, then Daisy is riding her bike,” to be true in the case where it is raining and Daisy is riding her bike.
4. Finally, suppose that both P and Q are false. That is, it is raining and Daisy is not riding her bike. As in the previous situation, since my statement was $P \to Q$, I made no claim about what would happen if it was raining, and so I did not tell a lie. So the statement $P \to Q$ cannot be false in this case and so we consider it to be true.

Progress Check 1.4: xplorations with Conditional Statements

1. Consider the following sentence:

If x is a positive real number, then $x^2 + 8x$ is a positive real number.

Although the hypothesis and conclusion of this conditional sentence are not statements, the conditional sentence itself can be considered to be a statement as long as we know what possible numbers may be used for the variable x. From the context of this sentence, it seems that we can substitute any positive real number for x. We can also substitute 0 for x or a negative real number for x provided that we are willing to work with a false hypothesis in the conditional statement. (In Chapter **2**, we will learn how to be more careful and precise with these types of conditional statements.)

(a) Notice that if $x = -3$, then $x^2 + 8x = -15$, which is negative. Does this mean that the given conditional statement is false?

(b) Notice that if $x = 4$, then $x^2 + 8x = 48$, which is positive. Does this mean that the given conditional statement is true?

(c) Do you think this conditional statement is true or false? Record the results for at least five different examples where the hypothesis of this conditional statement is true.

2. “If n is a positive integer, then $n^2 - n + 41$ is a prime number.” (Remember that a prime number is a positive integer greater than 1 whose only positive factors are 1 and itself.)
To explore whether or not this statement is true, try using (and recording your results) for $n = 1$, $n = 2$, $n = 3$, $n = 4$, $n = 5$, and $n = 10$. Then record the results for at least four other values of n. Does this conditional statement appear to be true?

Answer

Add texts here. Do not delete this text first.

Further Remarks about Conditional Statements

1. The conventions for the truth value of conditional statements may seem a bit strange,especially the fact that the conditional statement is true when the hypothesis of the conditional statement is false. The following example is meant to show that this makes sense.

   Suppose that Ed has exactly $52 in his wallet. The following four statements will use the four possible truth combinations for the hypothesis and conclusion of a conditional statement.

- If Ed has exactly \$52 in his wallet, then he has \$20 in his wallet. This is a true statement. Notice that both the hypothesis and the conclusion are true.
- If Ed has exactly \$52 in his wallet, then he has \$100 in his wallet. This statement is false. Notice that the hypothesis is true and the conclusion is false.
- If Ed has \$100 in his wallet, then he has at least \$50 in his wallet. This statement is true regardless of how much money he has in his wallet. In this case, the hypothesis is false and the conclusion is true.
- If Ed has \$100 in his wallet, then he has at least \$80 in his wallet. This statement is true regardless of how much money he has in his wallet. In this case, the hypothesis is false and the conclusion is false.

This is admittedly a contrived example but it does illustrate that the conventions for the truth value of a conditional statement make sense. The message is that in order to be complete in mathematics, we need to have conventions about when a conditional statement is true and when it is false.

2. The fact that there is only one case when a conditional statement is false often provides a method to show that a given conditional statement is false. In Progress Check **1.4**, you were asked if you thought the following conditional statement was true or false.

   If n is a positive integer, then $(n^2 - n + 41)$ is a prime number.

   Perhaps for all of the values you tried for n, $(n^2 - n + 41)$ turned out to be a prime number. However, if we try $n = 41$, we ge

   $$n^2 - n + 41 = 41^2 - 41 + 41$$
   $$n^2 - n + 41 = 41^2$$

   So in the case where $n = 41$, the hypothesis is true (41 is a positive integer) and the conclusion is false 41^2 is not prime. Therefore, 41 is a counterexample for this conjecture and the conditional statement
   "If n is a positive integer, then $(n^2 - n + 41)$ is a prime number"
   is false. There are other counterexamples (such as $n = 42$, $n = 45$, and $n = 50$), but only one counterexample is needed to prove that the statement is false.

3. Although one example can be used to prove that a conditional statement is false, in most cases, we cannot use examples to prove that a conditional statement is true. For example, in Progress Check **1.4**, we substituted values for x for the conditional statement "If x is a positive real number, then $x^2 + 8x$ is a positive real number." For every positive real number used for x, we saw that $x^2 + 8x$ was positive. However, this does not prove the conditional statement to be true because it is impossible to substitute every positive real number for x. So, although we may believe this statement is true, to be able to conclude it is true, we need to write a mathematical proof. Methods of proof will be discussed in Section **1.2** and Chapter **3**.

? Progress Check 1.5: Working with a Conditional Statement

The following statement is a true statement, which is proven in many calculus texts.

If the function f is differentiable at a, then the function f is continuous at a.

Using only this true statement, is it possible to make a conclusion about the function in each of the following cases?

1. It is known that the function f, where $f(x) = \sin x$, is differentiable at 0.
2. It is known that the function f, where $f(x) = \sqrt[3]{x}$, is not differentiable at 0.
3. It is known that the function f, where $f(x) = |x|$, is continuous at 0.
4. It is known that the function f, where $f(x) = \dfrac{|x|}{x}$ is not continuous at 0.

Answer

Add texts here. Do not delete this text first.

Closure Properties of Number Systems

The primary number system used in algebra and calculus is the **real number system**. We usually use the symbol R to stand for the set of all real numbers. The real numbers consist of the rational numbers and the irrational numbers. The **rational numbers** are those real numbers that can be written as a quotient of two integers (with a nonzero denominator), and the **irrational numbers** are those real numbers that cannot be written as a quotient of two integers. That is, a rational number can be written in the form of a fraction, and an irrational number cannot be written in the form of a fraction. Some common irrational numbers are $\sqrt{2}$, π and e. We usually use the symbol $\mathbb{Q}$ to represent the set of all rational numbers. (The letter $\mathbb{Q}$ is used because rational numbers are quotients of integers.) There is no standard symbol for the set of all irrational numbers.

Perhaps the most basic number system used in mathematics is the set of **natural numbers**. The natural numbers consist of the positive whole numbers such as 1, 2, 3, 107, and 203. We will use the symbol $\mathbb{N}$ to stand for the set of natural numbers. Another basic number system that we will be working with is the set of **integers**. The integers consist of zero, the positive whole numbers, and the negatives of the positive whole numbers. If n is an integer, we can write $n = \dfrac{n}{1}$. So each integer is a rational number and hence also a real number.

We will use the letter $\mathbb{Z}$ to stand for the set of integers. (The letter $\mathbb{Z}$ is from the German word, $Zahlen$, for numbers.) Three of the basic properties of the integers are that the set $\mathbb{Z}$ is **closed under addition**, the set $\mathbb{Z}$ is **closed under multiplication**, and the set of integers is **closed under subtraction.** This means that

- If x and y are integers, then $x + y$ is an integer;
- If x and y are integers, then $x \cdot y$ is an integer; and
- If x and y are integers, then $x - y$ is an integer.

Notice that these so-called closure properties are defined in terms of conditional statements. This means that if we can find one instance where the hypothesis is true and the conclusion is false, then the conditional statement is false.

✓ Example 1.6: Closure

1. In order for the set of natural numbers to be closed under subtraction, the following conditional statement would have to be true: If x and y are natural numbers, then $x - y$ is a natural number. However, since 5 and 8 are natural numbers, $5 - 8 = -3$, which is not a natural number, this conditional statement is false. Therefore, the set of natural numbers is not closed under subtraction.
2. We can use the rules for multiplying fractions and the closure rules for the integers to show that the rational numbers are closed under multiplication. If $\dfrac{a}{b}$ and $\dfrac{c}{d}$ are rational numbers (so a, b, c, and d are integers and b and d are not zero), then

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Since the integers are closed under multiplication, we know that ac and bd are integers and since $b \neq 0$ and $d \neq 0$, $bd \neq 0$. Hence, $\dfrac{ac}{bd}$ is a rational number and this shows that the rational numbers are closed under multiplication.

? Progress Check 1.7: Closure Properties

Answer each of the following questions.

1. Is the set of rational numbers closed under addition? Explain.
2. Is the set of integers closed under division? Explain.
3. Is the set of rational numbers closed under subtraction? Explain.

Answer

Add texts here. Do not delete this text first.

? 1.1

1. Which of the following sentences are statements?
   (a) $3^2 + 4^2 = 5^2$.
   (b) $a^2 + b^2 = c^2$.
   (c) There exists integers a, b, and c such that $a^2 + b^2 = c^2$.
   (d) If $x^2 = 4$, then $x = 2$.

(e) For each real number x, if $x^2 = 4$, then $x = 2$.
(f) For each real number t, $\sin^2 t + \cos^2 t = 1$.
(g) $\sin x < \sin(\frac{\pi}{4})$.
(h) If n is a prime number, then n^2 has three positive factors.
(i) $1 + \tan^2 \theta = \sec^2\theta$.
(j) Every rectangle is a parallelogram.
(k) Every even natural number greater than or equal to 4 is the sum of two prime numbers.

2. Identify the hypothesis and the conclusion for each of the following conditional statements.
   (a) If n is a prime number, then n^2 has three positive factors.
   (b) If a is an irrational number and b is an irrational number, then $a \cdot b$ is an irrational number.
   (c) If p is a prime number, then $p = 2$ or p is an odd number.
   (d) If p is a prime number and $p \neq 2$ or p is an odd number.
   (e) $p \neq 2$ or p is a even number, then p is not prime.
3. Determine whether each of the following conditional statements is true or false.
   (a) If 10 < 7, then 3 = 4.
   (b) If 7 < 10, then 3 = 4.
   (c) If 10 < 7, then 3 + 5 = 8.
   (d) If 7 < 10, then 3 + 5 = 8.
4. Determine the conditions under which each of the following conditional sentences will be a true statement.
   (a) If a + 2 = 5, then 8 < 5.
   (b) If 5 < 8, then a + 2 = 5.
5. Let P be the statement “Student X passed every assignment in Calculus I,” and let Q be the statement “Student X received a grade of C or better in Calculus I.”
   (a) What does it mean for P to be true? What does it mean for Q to be true?
   (b) Suppose that Student X passed every assignment in Calculus I and received a grade of B-, and that the instructor made the statement $P \to Q$. Would you say that the instructor lied or told the truth?
   (c) Suppose that Student X passed every assignment in Calculus I and received a grade of C-, and that the instructor made the statement $P \to Q$. Would you say that the instructor lied or told the truth?
   (d) Now suppose that Student X did not pass two assignments in Calculus I and received a grade of D, and that the instructor made the statement $P \to Q$. Would you say that the instructor lied or told the truth?
   (e) How are Parts (**5b**), (**5c**), and (**5d**) related to the truth table for $P \to Q$?
6. Following is a statement of a theorem which can be proven using calculus or precalculus mathematics. For this theorem, a, b, and c are real numbers.

   Theorem If f is a quadratic function of the form
   $f(x) = ax^2 + bx + c$ and a < 0, then the function f has a maximum value when $x = \dfrac{-b}{2a}$.

   Using **only** this theorem, what can be concluded about the functions given by the following formulas?
   (a) $g(x) = -8x^2 + 5x - 2$
   (b) $h(x) = -\dfrac{1}{3}x^2 + 3x$
   (c) $k(x) = 8x^2 - 5x - 7$
   (d) $j(x) = -\dfrac{71}{99}x^2 + 210$
   (e) $f(x) = -4x^2 - 3x + 7$
   (f) $F(x) = -x^4 + x^3 + 9$
7. Following is a statement of a theorem which can be proven using the quadratic formula. For this theorem, a, b, and c are real numbers.

   Theorem If f is a quadratic function of the form
   $f(x) = ax^2 + bx + c$ and ac < 0, then the function f has two x-intercepts.

   Using **only** this theorem, what can be concluded about the functions given by the following formulas?
   (a) $g(x) = -8x^2 + 5x - 2$

(b) $h(x) = -\frac{1}{3}x^2 + 3x$
(c) $k(x) = 8x^2 - 5x - 7$
(d) $j(x) = -\frac{71}{99}x^2 + 210$
(e) $f(x) = -4x^2 - 3x + 7$
(f) $F(x) = -x^4 + x^3 + 9$

8. Following is a statement of a theorem about certain cubic equations.For this theorem, b represents a real number.

   Theorem A. If f is a cubic function of the form $f(x) = x^3 - x + b$ and b > 1, then the function f has exactly one x-intercept.

   Following is another theorem about x-intercepts of functions:

   Theorem B. If f and g are functions with $g(x) = k \cdot f(x)$, where k is a nonzero real number, then f and g have exactly the same x-intercepts.

   Using only these two theorems and some simple algebraic manipulations, what can be concluded about the functions given by the following formulas?
   (a) $f(x) = x^3 - x + 7$
   (b) $g(x) = x^3 + x + 7$
   (c) $h(x) = -x^3 + x - 5$
   (d) $k(x) = 2x^3 + 2x + 3$
   (e) $r(x) = x^4 - x + 11$
   (f) $F(x) = 2x^3 - 2x + 7$

9. **(a)** Is the set of natural numbers closed under division?
   (b) Is the set of rational numbers closed under division?
   (c) Is the set of nonzero rational numbers closed under division?
   (d) Is the set of positive rational numbers closed under division?
   (e) Is the set of positive real numbers closed under subtraction?
   (f) Is the set of negative rational numbers closed under division?
   (g) Is the set of negative integers closed under addition?

   Explorations and Activities

10. **Exploring Propositions**. In Progress Check **1.2**, we used exploration to show that certain statements were false and to make conjectures that certain statements were true. We can also use exploration to formulate a conjecture that we believe to be true. For example, if we calculate successive powers of $2, (2^1, 2^2, 2^3, 2^4, 2^5, \ldots)$ and examine the units digits of these numbers, we could make the following conjectures (among others):
    - If n is a natural number, then the units digit of 2^n must be 2, 4, 6, or 8.
    - The units digits of the successive powers of 2 repeat according to the pattern “2, 4, 8, 6.”

    (a) Is it possible to formulate a conjecture about the units digits of successive powers of $4(4^1, 4^2, 4^3, 4^4, 4^5, \ldots)$? If so, formulate at least one conjecture.
    (b) Is it possible to formulate a conjecture about the units digit of numbers of the form $7^n - 2^n$, where n is a natural number? If so, formulate a conjecture in the form of a conditional statement in the form “If n is a natural number, then ... .”
    (c) Let $f(x) = e^{(}2x)$. Determine the first eight derivatives of this function. What do you observe? Formulate a conjecture that appears to be true. The conjecture should be written as a conditional statement in the form, “If n is a natural number, then ... .”

Answer

Add texts here. Do not delete this text first.

This page titled 1.1: Statements and Conditional Statements is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

1.2: Constructing Direct Proofs

Preview Activity 1 (Definition of Even and Odd Integers)

Definitions play a very important role in mathematics. A direct proof of a proposition in mathematics is often a demonstration that the proposition follows logically from certain definitions and previously proven propositions. A **definition** is an agreement that a particular word or phrase will stand for some object, property, or other concept that we expect to refer to often. In many elementary proofs, the answer to the question, "How do we prove a certain proposition?", is often answered by means of a definition. For example, in Progress Check **1.2** on page **5**, all of the examples you tried should have indicated that the following conditional statement is true:

If x and y are odd integers, then $x \cdot y$ is an odd integer.

In order to construct a mathematical proof of this conditional statement, we need a precise definition what it means to say that an integer is an even integer and what it means to say that an integer is an odd integer.

Definition

An integer a is an **even integer** provided that there exists an integer n such that $a = 2n$. An integer a is an **odd integer** provided there exists an integer n such that $a = 2n + 1$.

Using this definition, we can conclude that the integer 16 is an even integer since 16 = 2 ⋅ 8 and 8 is an integer. By answering the following questions, you should obtain a better understanding of these definitions. These questions are not here just to have questions in the textbook. Constructing and answering such questions is a way in which many mathematicians will try to gain a better understanding of a definition.

1. Use the definition given above to
   (a) Explain why 28, -42, 24, and 0 are even integers.
   (b) Explain why 51, -11, 1, and -1 are odd integers.

   It is important to realize that mathematical definitions are not made randomly. In most cases, they are motivated by a mathematical concept that occurs frequently.
2. Are the definitions of even integers and odd integers consistent with your previous ideas about even and odd integers?

Preview Activity 2 (Thinking about a Proof)

Consider the following proposition:

Proposition. If x and y are odd integers, then $x \cdot y$ is an odd integer.

Think about how you might go about proving this proposition. A **direct proof** of a conditional statement is a demonstration that the conclusion of the conditional statement follows logically from the hypothesis of the conditional statement. Definitions and previously proven propositions are used to justify each step in the proof. To help get started in proving this proposition, answer the following questions:

1. The proposition is a conditional statement. What is the hypothesis of this conditional statement? What is the conclusion of this conditional statement?
2. If $x = 2$ and $y = 3$, then $x \cdot y = 6$. Does this example prove that the proposition is false? Explain.
3. If $x = 5$ and $y = 3$, then $x \cdot y = 15$. Does this example prove that the proposition is true? Explain.

   In order to prove this proposition, we need to prove that whenever both x and y are odd integers, $x \cdot y$ is an odd integer. Since we cannot explore all possible pairs of integer values for x and y, we will use the definition of an odd integer to help us construct a proof.
4. To start a proof of this proposition,we will assume that the hypothesis of the conditional statement is true. So in this case, we assume that both x and yare odd integers. We can then use the definition of an odd integer to conclude that there exists an integer m such that $x = 2m + 1$. Now use the definition of an odd integer to make a conclusion about the integer y.

   Note: The definition of an odd integer says that a certain other integer exists. This definition may be applied to both x and y. However, do not use the same letter in both cases. To do so would imply that $x = y$ and we have not made that assumption. To be more specific, if $x = 2m + 1$ and $y = 2m + 1$, then $x = y$.

5. We need to prove that if the hypothesis is true, then the conclusion is true. So, in this case, we need to prove that $x \cdot y$ is an odd integer. At this point, we usually ask ourselves a so-called **backward question**. In this case, we ask, "Under what conditions can we conclude that $x \cdot y$ is an odd integer?" Use the definition of an odd integer to answer this question, and be careful to use a different letter for the new integer than was used in Part (**4**).

Properties of Number Systems

At the end of Section **1.1**, we introduced notations for the standard number systems we use in mathematics. We also discussed some closure properties of the standard number systems. For this text, it is assumed that the reader is familiar with these closure properties and the basic rules of algebra that apply to all real numbers. That is, it is assumed the reader is familiar with the properties of the real numbers shown in Table **1.2**.

Constructing a Proof of a Conditional Statement

In order to prove that a conditional statement $P \to Q$ is true, we only need to prove that Q is true whenever P is true. This is because the conditional statement is true whenever the hypothesis is false. So in a direct proof of $P \to Q$, we assume that P is true, and using this assumption, we proceed through a logical sequence of steps to arrive at the conclusion that Q is true.

Unfortunately, it is often not easy to discover how to start this logical sequence of steps or how to get to the conclusion that Q is true. We will describe a method of exploration that often can help in discovering the steps of a proof. This method will involve working forward from the hypothesis, P, and backward from the conclusion, Q. We will use a device called the "**know-show table**" to help organize our thoughts and the steps of the proof. This will be illustrated with the proposition from Preview Activity **2**.

For all real numbers x, y and z

Identity Properties	$x + 0 = x$ and $x \cdot 1 = x$
Inverse Properties	$x + (-x) = 0$ and if $x \neq 0$, then $x \cdot \frac{1}{x} = 1$.
Commutative Properties	$x + y = y + x$ and $xy = yx$
Associative Properties	$(x + y) + z = x + (y + z)$ and $(xy)z = x(yz)$
Distributive Properties	$x(y + z) = xy + xz$ and $(y + z)x = yx + zx$

Table 1.2: Properties of the Real Numbers

Proposition. If x and y are odd integers, then $x \cdot y$ is an odd integer.
The first step is to identify the hypothesis, P, and the conclusion,Q, of the conditional statement. In this case, we have the following:

P : x and y are odd integers. Q: $x \cdot y$ is an odd integer.

We now treat P as what we know (we have assumed it to be true) and treat Q as what we want to show (that is, the goal). So we organize this by using P as the first step in the know portion of the table and Q as the last step in the show portion of the table. We will put the know portion of the table at the top and the show portion of the table at the bottom.

Step	**Know**	**Reason**
P	x and y are odd integers	Hypothesis
$P1$	...	...
...	...	...
$Q1$	...	...
Q	$x \cdot y$ is an odd integer.	?
Step	**Show**	**Reason**

We have not yet filled in the reason for the last step because we do not yet know how we will reach the goal. The idea now is to ask ourselves questions about what we know and what we are trying to prove. We usually start with the conclusion that we are trying to prove by asking a so-called **backward question**. The basic form of the question is, “Under what conditions can we conclude that Q is true?” How we ask the question is crucial since we must be able to answer it. We should first try to ask and answer the question in an abstract manner and then apply it to the particular form of statement Q.

In this case, we are trying to prove that some integer is an odd integer. So our backward question could be, “How do we prove that an integer is odd?” At this time, the only way we have of answering this question is to use the definition of an odd integer. So our answer could be, “We need to prove that there exists an integer q such that the integer equals $2q + 1$.” We apply this answer to statement Q and insert it as the next to last line in the know-show table.

Step	**Know**	**Reason**
P	x and y are odd integers	Hypothesis
$P1$	...	...
...	...	...
$Q1$	There exists an integer q such that $xy = 2q + 1$	...
Q	$x \cdot y$ is an odd integer.	Definition of an odd integer
Step	**Show**	**Reason**

We now focus our effort on proving statement $Q1$ since we know that if we can prove $Q1$, then we can conclude that Q is true. We ask a backward question about $Q1$ such as, “How can we prove that there exists an integer q such that $x \cdot y = 2q + 1$?” We may not have a ready answer for this question, and so we look at the know portion of the table and try to connect the know portion to the show portion. To do this, we work forward from step P, and this involves asking a **forward question**. The basic form of this type of question is, “What can we conclude from the fact that P is true?” In this case, we can use the definition of an odd integer to conclude that there exist integers m and n such that $x = 2m + 1$ and $y = 2n + 1$. We will call this Step $P1$ in the know-show table. It is important to notice that we were careful not to use the letter q to denote these integers. If we had used q again, we would be claiming that the same integer that gives $x \cdot y = 2q + 1$ also gives $x = 2q + 1$. This is why we used m and n for the integers x and y since there is no guarantee that x equals y. The basic rule of thumb is to use a different symbol for each new object we introduce in a proof. So at this point, we have:

- Step $P1$. We know that there exist integers m and n such that $x = 2m + 1$ and $y = 2n + 1$.
- Step $Q1$. We need to prove that there exists an integer q such that $x \cdot y = 2q + 1$.

We must always be looking for a way to link the “know part” to the “show part”. There are conclusions we can make from $P1$, but as we proceed, we must always keep in mind the form of statement in $Q1$. The next forward question is, “What can we conclude about $x \cdot y$from what we know?” One way to answer this is to use our prior knowledge of algebra. That is, we can first use substitution to write $x \cdot y = (2m + 1)(2n + 1)$. Although this equation does not prove that $x \cdot y$ is odd, we can use algebra to try to rewrite the right side of this equation. $(2m + 1)(2n + 1)$ in the form of an odd integer so that we can arrive at step $Q1$. We first expand the right side of the equation to obtain

$$x \cdot y = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1$$

Now compare the right side of the last equation to the right side of the equation in step $Q1$. Sometimes the difficult part at this point is the realization that q stands for some integer and that we only have to show that $x \cdot y$ equals two times some integer plus one. Can we now make that conclusion? The answer is yes because we can factor a 2 from the first three terms on the right side of the equation and obtain

$$x \cdot y = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1$$

We can now complete the table showing the outline of the proof as follows:

Step	**Know**	**Reason**
P	x and y are odd integers	Hypothesis

$P1$	There exist integers m and n such that $x = 2m+1$ and $y = 2n+1$.	Definition of an odd integer.
$P2$	$xy = (2m+1)(2n+1)$	Substitution
$P3$	$xy = 4mn+2m+2n+1$	Algebra
$P4$	$xy = 2(2mn+m+n)+1$	Algebra
$P5$	$(2mn+m+n)$ is an integer	Closure properties of the integers
$Q1$	There exists an integer q such that $xy = 2q+1$	Use $q = (2mn+m+n)$
Q	$x \cdot y$ is an odd integer.	Definition of an odd integer

It is very important to realize that we have only constructed an outline of a proof. Mathematical proofs are not written in table form. They are written in narrative form using complete sentences and correct paragraph structure, and they follow certain conventions used in writing mathematics. In addition, most proofs are written only from the forward perspective. That is, although the use of the backward process was essential in discovering the proof, when we write the proof in narrative form, we use the forward process described in the preceding table. A completed proof follows.

Theorem

If x and y are odd integers, then $x \cdot y$ is an odd integer.

Proof

We assume that x and y are odd integers and will prove that $x \cdot y$ is an odd integer. Since x and y are odd, there exist integers m and n such that

$$x = 2m+1 \text{ and } y = 2n+1.$$

Using algebra, we obtain

$$x \cdot y = (2m+1)(2n+1) = 4mn+2m+2n+1 = 2(2mn+m+n)+1$$

Since m and n are integers and the integers are closed under addition and multiplication, we conclude that $2mn+m+n$ is an integer. This means that $x \cdot y$ has been written in the form $2q+1$ for some integer q, and hence, $x \cdot y$ is an odd integer. Consequently, it has been proven that if x and y are odd integers, then $x \cdot y$ is an odd integer.

Writing Guidelines for Mathematics Proofs

At the risk of oversimplification, doing mathematics can be considered to have two distinct stages. The first stage is to convince yourself that you have solved the problem or proved a conjecture. This stage is a creative one and is quite often how mathematics is actually done. The second equally important stage is to convince other people that you have solved the problem or proved the conjecture. This second stage often has little in common with the first stage in the sense that it does not really communicate the process by which you solved the problem or proved the conjecture. However, it is an important part of the process of communicating mathematical results to a wider audience.

A **mathematical proof** is a convincing argument (within the accepted standards of the mathematical community) that a certain mathematical statement is necessarily true. A proof generally uses deductive reasoning and logic but also contains some amount of ordinary language (such as English). A mathematical proof that you write should convince an appropriate audience that the result you are proving is in fact true. So we do not consider a proof complete until there is a well-written proof. So it is important to introduce some writing guidelines. The preceding proof was written according to the following basic guidelines for writing proofs. More writing guidelines will be given in Chapter 3.

1. **Begin with a carefully worded statement of the theorem or result to be proven.** This should be a simple declarative statement of the theorem or result. Do not simply rewrite the problem as stated in the textbook or given on a handout. Problems often begin with phrases such as “Show that” or “Prove that.” This should be reworded as a simple declarative statement of the

theorem. Then skip a line and write “Proof” in italics or boldface font (when using a word processor). Begin the proof on the same line. Make sure that all paragraphs can be easily identified. Skipping a line between paragraphs or indenting each paragraph can accomplish this.

As an example, an exercise in a text might read, “Prove that if x is an odd integer, then x^2 is an odd integer.” This could be started as follows:

Theorem

If x is an odd integer, then x^2 is an odd integer.

Proof

We assume that x is an odd integer ...

2. **Begin the proof with a statement of your assumptions.** Follow the statement of your assumptions with a statement of what you will prove.

Theorem 1.2.1

If x is an odd integer, then x^2 is an odd integer.

Proof

We assume that x is an odd integer and will prove that x^2 is an odd integer.

3. **Usethepronoun“we.”** If a pronoun is used in a proof, the usual convention is to use “we” instead of “I.” The idea is to stress that you and the reader are doing the mathematics together. It will help encourage the reader to continue working through the mathematics. Notice that we started the proof of Theorem **1.8** with “We assume that... .”
4. **Use italics for variables when using a word processor.** When using a word processor to write mathematics, the word processor needs to be capable of producing the appropriate mathematical symbols and equations. The mathematics that is written with a word processor should look like typeset mathematics. This means that italics font is used for variables, boldface font is used for vectors, and regular font is used for mathematical terms such as the names of the trigonometric and logarithmic functions.

   For example, we do not write $sin\,x$ or $\mathbf{sin}\,x$. The proper way to typeset this is $\sin x$.

5. **Display important equations and mathematical expressions.** Equations and manipulations are often an integral part of mathematical exposition. Do not write equations, algebraic manipulations, or formulas in one column with reasons given in another column. Important equations and manipulations should be displayed. This means that they should be centered with blank lines before and after the equation or manipulations, and if the left side of the equations do not change, it should not be repeated. For example,

   Using algebra, we we obtain

   $$x \cdot y = (2m+1)(2n+1) = 4mn+2m+2n+1 = 2(2mn+m+n)+1$$

   Since m and n are integers, we conclude that ... .

6. Tell the reader when the proof has been completed. Perhaps the best way to do this is to simply write, “This completes the proof.” Although it may seem repetitive, a good alternative is to finish a proof with a sentence that states precisely what has been proven. In any case, it is usually good practice to use some “end of proof symbol” such as

? Progress Check 1.9 (Proving Propositions)

Construct a know-show table for each of the following propositions and then write a formal proof for one of the propositions.

1. If x is an even integer and y is an even integer, then $x+y$ is an even integer.
2. If x is an even integer and y is an odd integer, then $x+y$ is an odd integer.
3. If x is an even integer and y is an odd integer, then $x+y$ is an even integer.

Answer

Some Comments about Constructing Direct Proofs

1. When we constructed the know-show table prior to writing a proof for Theorem **1.8**, we had only one answer for the backward question and one answer for the forward question. Often, there can be more than one answer for these questions. For example, consider the following statement:

   If x is an odd integer, then x^2 is an odd integer.

   The backward question for this could be, “How do I prove that an integer is an odd integer?” One way to answer this is to use the definition of an odd integer, but another way is to use the result of Theorem **1.8**. That is, we can prove an integer is odd by proving that it is a product of two odd integers.

   The difficulty then is deciding which answer to use. Sometimes we can tell by carefully watching the interplay between the forward process and the backward process. Other times, we may have to work with more than one possible answer.

2. Sometimes we can use previously proven results to answer a forward question or a backward question. This was the case in the example given in Comment (**1**), where Theorem **1.8** was used to answer a backward question.
3. Although we start with two separate processes (forward and backward), the key to constructing a proof is to find a way to link these two processes. This can be difficult. One way to proceed is to use the know portion of the table to motivate answers to backward questions and to use the show portion of the table to motivate answers to forward questions.
4. Answering a backward question can sometimes be tricky. If the goal is the statement Q, we must construct the know-show table so that if we know that $Q1$ is true, then we can conclude that Q is true. It is sometimes easy to answer this in a way that if it is known that Q is true, then we can conclude that $Q1$ is true. For example, suppose the goal is to prove

   $$y^2 = 4,$$

   where y is a real number. A backward question could be, “How do we prove the square of a real number equals four?” One possible answer is to prove that the real number equals 2. Another way is to prove that the real number equals 2. This is an appropriate backward question, and these are appropriate answers.

   However, if the goal is to prove

   $$y = 2$$

   where y is a real number, we could ask, “How do we prove a real number equals 2?” It is not appropriate to answer this question with “prove that the square of the real number equals 4.” This is because if $y^2 = 4$, then it is not necessarily true that $y = 2$.

5. Finally,it is very important to realize that not every proof can be constructed by the use of a simple know-show table. Proofs will get more complicated than the ones that are in this section. The main point of this section is not the know-show table itself, but the way of thinking about a proof that is indicated by a know-show table. In most proofs, it is very important to specify carefully what it is that is being assumed and what it is that we are trying to prove. The process of asking the “backward questions” and the “forward questions” is the important part of the know-show table. It is very important to get into the “habit of mind” of working backward from what it is we are trying to prove and working forward from what it is we are assuming. Instead of immediately trying to write a complete proof, we need to stop, think, and ask questions such as

- Just exactly what is it that I am trying to prove?
- How can I prove this?
- What methods do I have that may allow me to prove this?
- What are the assumptions?
- How can I use these assumptions to prove the result?

Progress Check 1.10 (Exploring a Proposition)

Construct a table of values for $3m^2+4m+6$ using at least six different integers for m. Make one-half of the values for m even integers and the other half odd integers. Is the following proposition true or false?

If m is an odd integer, then $3m^2+4m+6$ is an odd integer.

Justify your conclusion. This means that if the proposition is true, then you should write a proof of the proposition. If the proposition is false, you need to provide an example of an odd integer for which $3m^2+4m+6$ is an even integer.

Answer

Add texts here. Do not delete this text first.

Progress Check 1.11 (Constructing and Writing a Proof)

The **Pythagorean Theorem** for right triangles states that if a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse, then $a^2+b^2=c^2$. For example, if $a=5$ and $b=12$ are the lengths of the two sides of a right triangle and if c is the length of the hypotenuse, then the $c^2=5^2+12^2$ and $c^2=169$. Since c is a length and must be positive, we conclude that $c=13$.

Construct and provide a well-written proof for the following proposition.

Proposition. If m is a real number and m, $m+1$, and $m+2$ are the lengths of the three sides of a right triangle, then $m=3$.

Although this proposition uses different mathematical concepts than the one used in this section, the process of constructing a proof for this proposition is the same forward-backward method that was used to construct a proof for Theorem **1.8**. However, the backward question, "How do we prove that $m=3$?" is simple but may be difficult to answer. The basic idea is to develop an equation from the forward process and show that $m=3$ is a solution of that equation.

Answer

Add texts here. Do not delete this text first.

Exercises for Section 1.2

1. Construct a know-show table for each of the following statements and then write a formal proof for one of the statements.

   (a) If m is an even integer,then $m+1$ is an odd integer.
   (b) If m is an odd integer, then $m+1$ is an even integer.
2. Construct a know-show table for each of the following statements and then write a formal proof for one of the statements.

   (a) If x is an even integer and y is an even integer, then $x+y$ is an even integer.
   (b) If x is an even integer and y is an odd integer, then $x+y$ is an odd integer.
   (c) If x is an odd integer and y is an odd integer, then $x+y$ is an even integer.
3. Construct a know-show table for each of the following statements and then write a formal proof for one of the statements.

   (a) If m is an even integer and n is an integer, then $m\cdot n$ is an even integer.
   (b) If n is an even integer, then n^2 is an even integer.
   (c) If n is an odd integer, then n^2 is an odd integer.
4. Construct a know-show table and write a complete proof for each of the following statements:

   (a) If m is an even integer, then $5m+7$ is an odd integer.
   (b) If m is an odd integer, then $5m+7$ is an even integer.
   (c) If m and n are odd integers, then $mn+7$ is an even integer.

5. Construct a know-show table and write a complete proof for each of the following statements:

   (a) If m is an even integer, then $3m^2+2m+3$ is an odd integer.
   (b) If m is an odd integer, then $3m^2+7m+12$ is an even integer.
6. In this section, it was noted that there is often more than one way to answer a backward question. For example, if the backward question is, “How can we prove that two real numbers are equal?”, one possible answer is to prove that their difference equals 0. Another possible answer is to prove that the first is less than or equal to the second and that the second is less than or equal to the first

   (a) Give at least one more answer to the backward question, “How can we prove that two real numbers are equal?”
   (b) List as many answers as you can for the backward question, “How can we prove that a real number is equal to zero?”
   (c) List as many answers as you can for the backward question, “How can we prove that two lines are parallel?”
   (d) List as many answers as you can for the backward question, “How can we prove that a triangle is isosceles?”
7. Are the following statements true or false? Justify your conclusions.

   (a) If a, b and c are integers, then $ab+ac$ is an even integer.
   (b) If b and c are odd integers and a is an integer, then $ab+ac$ is an even integer.
8. Is the following statement true or false? Justify your conclusion.
   If a and b are nonnegative real numbers and $a+b=0$, then $a=0$.

   Either give a counterexample to show that it is false or outline a proof by completing a know-show table.
9. An integer a is said to be a **type 0 integer** if there exists an integer n such that $a=3n$. An integer a is said to be a **type 1 integer** if there exists an integer n such that $a=3n+1$. An integer a is said to be a **type 2 integer** if there exists an integer m such that $a=3m+2$.

   (a) Give examples of at least four different integers that are type 1 integers.
   (b) Give examples of at least four different integers that are type 2 integers.
   (c) By multiplying pairs of integers from the list in Exercise (9a), does it appear that the following statement is true or false?

   If a and b are both type 1 integers, then $a \cdot b$ is a type 1 integer.
10. Use the definitions in Exercise (9) to help write a proof for each of the following statements:

    (a) If a and b are both type 1 integers, then $a+b$ is a type 2 integer.
    (b) If a and b are both type 2 integers, then $a+b$ is a type 1 integer.
    (a) If a is a type 1 integer and b is a type 2 integer, then $a \cdot b$ is a type 2 integer.
    (a) If a and b are both type 2 integers, then $a \cdot b$ is type 1 integer.
11. Let a, b, and c be real numbers with $a \neq 0$. The solutions of the **quadratic equation** $ax^2+bx+c=0$ are given by the **quadratic formula**, which states that the solutions are $x1$ and $x2$, where

    $$x_1 = \frac{-b+\sqrt{(b^2-4ac)}}{2a} \text{ and } x_2 = \frac{-b-\sqrt{(b^2-4ac)}}{2a}.$$

    (a) Prove that the sum of the two solutions of the quadratic equation $ax^2+bx+c=0$ is equal to $-\frac{b}{a}$.
    (b) Prove that the product of the two solutions of the quadratic equation $ax^2+bx+c=0$ is equal to $\frac{c}{a}$.
12. (a) See Exercise (**11**) for the quadratic formula, which gives the solutions to a quadratic equation. Let a, b, and c be real numbers with $a \neq 0$. The discriminant of the quadratic equation $ax^2+bx+c=0$ is defined to be b^2-4ac. Explain how to use this discriminant to determine if the quadratic equation has two real number solutions, one real number solution, or no real number solutions.
    (b) Prove that if a, b, and c are real numbers with $a>0$ and $c<0$, then one solutions of the quadratic equation $ax^2+bx+c=0$ is a positive real number.
    (c) Prove that if a, b, and c are real numbers with $a \neq 0$, $b>0$, and $b<2\sqrt{(ac)}$, then the quadratic equation $ax^2+bx+c=0$ has no real number solutions.

Explorations and Activities

13. **Pythagorean Triples**. Three natural numbers a, b, and c with $a < b < c$ are said to form a **Pythagorean triple** provided that $a^2 + b^2 = c^2$. For example, 3, 4, and 5 form a Pythagorean triple since $3^2 + 4^2 = 5^2$. The study of Pythagorean triples began with the development of the **Pythagorean Theorem** for right triangles, which states that if a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse, then $a^2 + b^2 = c^2$. For example, if the lengths of the legs of a right triangle are 4 and 7 units, then $c^2 = 4^2 + 7^2 = 63$, and the length of the hypotenuse must be $\sqrt{63}$ units (since the length must be a positive real number). Notice that 4, 7, and $\sqrt{63}$ are not a Pythagorean triple since $\sqrt{63}$ is not a natural number.

    (a) Verify that each of the following triples of natural numbers form a Pythagorean triple.

    (1) 3, 4, and 5. (2) 8, 15, and 17. (3) 12, 35, and 37
    (4) 6, 8, and 10. (5) 10, 24, and 26 (6) 14, 48, and 50

    (b) Does there exist a Pythagorean triple of the form m, $m + 7$, and $m + 8$, where m is a natural number? If the answer is yes, determine all such Pythagorean triples. If the answer is no, prove that no such Pythagorean triple exists.

    (c) Does there exist a Pythagorean triple of the form m, $m + 11$,and $m + 12$, where m is a natural number? If the answer is yes, determine all such Pythagorean triples. If the answer is no, prove that no such Pythagorean triple exists.
14. **More Work with Pythagorean Triples**. In Exercise (**13**), we verified that each of the following triples of natural numbers are Pythagorean triples:

    (1) 3, 4, and 5. (2) 8, 15, and 17. (3) 12, 35, and 37
    (4) 6, 8, and 10. (5) 10, 24, and 26 (6) 14, 48, and 50

    (a) Focus on the least even natural number in each of these Pythagorean triples. Let n be this even number and find m so that $n = 2m$. Now try to write formulas for the other two numbers in the Pythagorean triple in terms of m. For example, for 3, 4, and 5, $n = 4$ and $m = 2$, and for 8, 15, and 17, $n = 8$ and $m = 4$. Once you think you have formulas, test your results with $m = 10$. That is, check to see that you have a Pythagorean triple whose smallest even number is 20.

    (b) Write a proposition and then write a proof of the proposition. The proposition should be in the form: If m is a natural number and $m \geq 2$, then ......

Answer

Add texts here. Do not delete this text first.

This page titled 1.2: Constructing Direct Proofs is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

1.S: Introduction to Writing Proofs in Mathematics (Summary)

Important Definitions

- Statement
- Odd integer
- Conditional statement
- Even integer
- Pythagorean triple

Important Number Systems and Their Properties

- The natural numbers, $\mathbb{N}$; the integers, $\mathbb{Z}$; the rational numbers, $\mathbb{Q}$; and the real number, $\mathbb{R}$.
- Closure Properties of the Number Systems

Number System	Closed Under
Natural numbers, $\mathbb{N}$	addition and multiplication
Integers, $\mathbb{Z}$	addition, subtraction, and multiplication
Rational numbers, $\mathbb{Q}$	addition, subtraction, and multiplication, and division by nonzero rational numbers
Real number, $\mathbb{R}$	addition, subtraction, and multiplication, and division by nonzero real numbers

- Inverse,commutative,associative, and distributive properties of the real numbers.

Important Theorems and Results

- **Exercise (1), Section 1.2**
  If m is an even integer, then $m+1$ is an odd integer.
  If m is an odd integer, then $m+1$ is an even integer.
- **Exercise (2), Section 1.2**
  If x is an even integer and y is an even integer, then $x+y$ is an even integer.
  If x is an even integer and y is an odd integer, then $x+y$ is an odd integer.
  If x is an odd integer and y is an odd integer, then $x+y$ is an even integer.
- **Exercise (3), Section 1.2.**
  If x is an even integer and y is an integer, then $x \cdot y$ is an even integer.
- **Theorem1.8**. If x is an odd integer and y is an odd integer, then $x \cdot y$ is an odd integer.
- The **Pythagorean Theorem**. If a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse, then $a^2 + b^2 = c^2$.

This page titled 1.S: Introduction to Writing Proofs in Mathematics (Summary) is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

CHAPTER OVERVIEW

2: Logical Reasoning

2.1: Statements and Logical Operators
2.2: Logically Equivalent Statements
2.3: Open Sentences and Sets
2.4: Quantifiers and Negations
2.S: Logical Reasoning (Summary)

Thumbnail: The "magic eight ball" is not an example of logical reasoning to get an answer to a problem. (CC BY 2.0 Generic; Atlasowa)

This page titled 2: Logical Reasoning is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

2.1: Statements and Logical Operators

PREVIEW ACTIVITY 2.1.1: Compound Statements

Mathematicians often develop ways to construct new mathematical objects from existing mathematical objects. It is possible to form new statements from existing statements by connecting the statements with words such as “and” and “or” or by negating the statement. A **logical operator** (or **connective**) on mathematical statements is a word or combination of words that combines one or more mathematical statements to make a new mathematical statement. A **compound statement** is a statement that contains one or more operators. Because some operators are used so frequently in logic and mathematics, we give them names and use special symbols to represent them.

- The conjunction of the statements P and Q is the statement “P **and** Q” and its denoted by $P \wedge Q$. The statement $P \wedge Q$ is true only when both P **and** Q are true.
- The **disjunction** of the statements P and Q is the statement “P **or** Q” and its denoted by $P \vee Q$. The statement $P \vee Q$ is true only when at least one of P or Q is true.
- The **negation** (**of a statement**) of the statement P is the statement “**not** P ” and is denoted by $\urcorner P$. The negation of P is true only when P is false, and $\urcorner P$ is false only when P is true.
- The **implication** or **conditional** is the statement “**If** P **then** Q” and is denoted by $P \rightarrow Q$. The statement $P \rightarrow Q$ is often read as “P **implies** Q, and we have seen in Section 1.1 that $P \rightarrow Q$ is false only when P is true and Q is false.

Some comments about the disjunction.
It is important to understand the use of the operator “or.” In mathematics, we use the “**inclusive or**” unless stated otherwise. This means that $P \vee Q$ is true when both P and Q are true and also when only one of them is true. That is, $P \vee Q$ is true when at least one of P or Q is true, or $P \vee Q$ is false only when both P and Q are false.

A different use of the word “or” is the “**exclusive or**.” For the exclusive or, the resulting statement is false when both statements are true. That is, “P exclusive or Q” is true only when exactly one of P or Q is true. In everyday life, we often use the exclusive or. When someone says, “At the intersection, turn left or go straight,” this person is using the exclusive or.

Some comments about the negation. Although the statement, $\urcorner P$, can be read as “It is not the case that P,” there are often betters ways to say or write this in English. For example, we would usually say (or write):

- The negation of the statement, “391 is prime” is “391 is not prime.”
- The negation of the statement, “$12 < 9$” is “$12 \geq 9$.”

1. For the statements

   P: 15 is odd Q: 15 is prime
   write each of the following statements as English sentences and determine

   whether they are true or false.
   (a) $P \wedge Q$. (b) $P \vee Q$. (c) $P \wedge \urcorner Q$. (d) $\urcorner P \vee \urcorner Q$.

2. For the statements

   P : 15 is odd R: 15 < 17

   write each of the following statements in symbolic form using the operators$\wedge$, $\vee$, and $\urcorner$

   (a) $15 \geq 17$. (b) 15 is odd or $15 \geq 17$.
   (c) 15 is even or 15 <17. (d) 15 is odd and $15 \geq 17$.

PREVIEW ACTIVITY2.1.2: Truth Values of Statements

We will use the following two statements for all of this Preview Activity:

- P is the statement “It is raining.”
- Q is the statement “Daisy is playing golf.”

In each of the following four parts, a truth value will be assigned to statements P and Q. For example, in Question (1), we will assume that each statement is true. In Question (2), we will assume that P is true and Q is false. In each part, determine the truth value of each of the following statements:

(a) $(P \wedge Q)$ It is raining and Daisy is playing golf.

(b) $(P \vee Q)$ It is raining or Daisy is playing golf.

(c) $(P \rightarrow Q)$ If it is raining, then Daisy is playing golf.

(d) $(\urcorner P)$ It is not raining.

Which of the four statements [(a) through (d)] are true and which are false in each of the following four situations?

1. When P is true (it is raining) and Q is true (Daisy is playing golf).
2. When P is true (it is raining) and Q is false (Daisy is not playing golf).
3. When P is false (it is not raining) and Q is true (Daisy is playing golf).
4. When P is false (it is not raining) and Q is false (Daisy is not playing golf).

In the preview activities for this section, we learned about compound statements and their truth values. This information can be summarized with truth tables as is shown below.

P	$\urcorner P$
T	F
F	T

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Rather than memorizing the truth tables, for many people it is easier to remember the rules summarized in Table 2.1.

Table 2.1: Truth Values for Common Connectives

Operator	**Symbolic Form**	**Summary of Truth Values**
Conjunction	$P \wedge Q$	True only when both P and Q are true

Operator	Symbolic Form	Summary of Truth Values
Disjunction	$P \vee Q$	False only when both P and Q are false
Negation	$\urcorner P$	Opposite truth value of P
Conditional	$P \to Q$	False only when P is true and Q is false

Other Forms of Conditional Statements

Conditional statements are extremely important in mathematics because almost all mathematical theorems are (or can be) stated in the form of a conditional statement in the following form:

If “certain conditions are met,” then “something happens.”

It is imperative that all students studying mathematics thoroughly understand the meaning of a conditional statement and the truth table for a conditional statement.

We also need to be aware that in the English language, there are other ways for expressing the conditional statement $P \to Q$ other than “If P, then Q.” Following are some common ways to express the conditional statement $P \to Q$ in the English language: page54image1422600880

- If P, then Q.
- P implies Q.
- P only if Q.
- Q if P.
- Whenever P is true, Q is true.
- Q is true whenever P is true.
- Q is necessary for P. (This means that if P is true, then Q is necessarily true.)
- P is sufficient for Q. (This means that if you want Q to be true, it is sufficient to show that P is true.)

In all of these cases, P is the **hypothesis** of the conditional statement and Q is the **conclusion** of the conditional statement.

? Progress Check 2.1: The "Only if" statemenT

Recall that a quadrilateral is a four-sided polygon. Let S represent the following true conditional statement:

If a quadrilateral is a square, then it is a rectangle.

Write this conditional statement in English using

1. the word “whenever”
2. the phrase “only if”
3. the phrase “is necessary for”
4. the phrase “is sufficient for”

Answer

Add texts here. Do not delete this text first.

Constructing Truth Tables

Truth tables for compound statements can be constructed by using the truth tables for the basic connectives. To illustrate this, we will construct a truth table for. $(P \wedge \urcorner Q) \to R$. The first step is to determine the number of rows needed.

- For a truth table with two different simple statements, four rows are needed since there are four different combinations of truth values for the two statements. We should be consistent with how we set up the rows. The way we will do it in this text is to label the rows for the first statement with (T, T, F, F) and the rows for the second statement with (T, F, T, F). All truth tables in the text have this scheme.
- For a truth table with three different simple statements, eight rows are needed since there are eight different combinations of truth values for the three statements. Our standard scheme for this type of truth table is shown in Table **2.2**.

The next step is to determine the columns to be used. One way to do this is to work backward from the form of the given statement. For $(P \wedge \urcorner Q) \rightarrow R$, the last step is to deal with the conditional operator $(\rightarrow)$. To do this, we need to know the truth values of $(P \wedge \urcorner Q)$ and R. To determine the truth values for $(P \wedge \urcorner Q)$, we need to apply the rules for the conjunction operator $(\wedge)$ and we need to know the truth values for P and $\urcorner Q$.

Table **2.2** is a completed truth table for $(P \wedge \urcorner Q) \rightarrow R$ with the step numbers indicated at the bottom of each column. The step numbers correspond to the order in which the columns were completed.

Table 2.2: Truth Table for $(P \wedge \urcorner Q) \rightarrow R$

P	Q	R	$\urcorner Q$	$(P \wedge \urcorner Q)$	$(P \wedge \urcorner Q) \rightarrow R$
T	T	T	F	F	T
T	T	F	F	F	T
T	F	T	T	T	T
T	F	F	T	T	F
F	T	T	F	F	T
F	T	F	F	F	T
F	F	T	T	F	T
F	F	F	T	F	T
1	1	1	2	3	4

- When completing the column for $P \wedge \urcorner Q$, remember that the only time the conjunction is true is when both P and $\urcorner Q$ are true.
- When completing the column for $(P \wedge \urcorner Q) \rightarrow R$, remember that the only time the conditional statement is false is when the hypothesis $(P \wedge \urcorner Q)$ is true and the conclusion, R, is false.

The last column entered is the truth table for the statement $(P \wedge \urcorner Q) \rightarrow R$ using the set up in the first three columns.

Progress Check 2.2: Constructing Truth Tables

Construct a truth table for each of the following statements:

1. $P \wedge \urcorner Q$
2. $\urcorner(P \wedge Q)$
3. $\urcorner P \wedge \urcorner Q$
4. $\urcorner P \vee \urcorner Q$

Do any of these statements have the same truth table?

Answer

Add texts here. Do not delete this text first.

The Biconditional Statement

Some mathematical results are stated in the form "P if and only if Q" or "P is necessary and sufficient for Q." An example would be, "A triangle is equilateral if and only if its three interior angles are congruent." The symbolic form for the biconditional statement "P if and only if Q" is $P \leftrightarrow Q$. In order to determine a truth table for a biconditional statement, it is instructive to look carefully at the form of the phrase "P if and only if Q." The word "and" suggests that this statement is a conjunction. Actually it is a conjunction of the statements "P if Q" and "P only if Q." The symbolic form of this conjunction is $[(Q \rightarrow P) \wedge (P \rightarrow Q]$.

Progress Check 2.3: The Truth Table for the Biconditional Statement

Complete a truth table for $[(Q \rightarrow P) \wedge (P \rightarrow Q]$. Use the following columns: P, Q, $Q \rightarrow P$, $P \rightarrow Q$, and $[(Q \rightarrow P) \wedge (P \rightarrow Q]$. The last column of this table will be the truth for $P \leftrightarrow Q$.

Answer

Add texts here. Do not delete this text first.

Other Forms of the Biconditional Statement

As with the conditional statement, there are some common ways to express the biconditional statement, $P \leftrightarrow Q$, in the English language.

Example

- P is and only if Q.
- P is necessary and sufficient for Q.
- P implies Q and Q implies P.

Tautologies and Contradictions

Definition: tautology

A **tautology** is a compound statement S that is true for all possible combinations of truth values of the component statements that are part of S. A **contradiction** is a compound statement that is false for all possible combinations of truth values of the component statements that are part of S.

That is, a tautology is necessarily true in all circumstances, and a contradiction is necessarily false in all circumstances.

Progress Check 2.4 (Tautologies and Contradictions)

For statements P and Q:

1. Use a truth table to show that $(P \vee \urcorner P)$ is a tautology.
2. Use a truth table to show that $(P \wedge \urcorner P)$ is a contradiction.
3. Use a truth table to determine if $P \rightarrow (P \vee P)$ is a tautology, a contradiction, nor neither.

Answer

Add texts here. Do not delete this text first.

Exercises for Section 2.1

1. Suppose that Daisy says, “If it does not rain, then I will play golf.” Later in the day you come to know that it did rain but Daisy still played golf. Was Daisy’s statement true or false? Support your conclusion.
2. Suppose that P and Q are statements for which $P \rightarrow Q$ is true and for which $\urcorner Q$ is true. What conclusion (if any) can be made about the truth value of each of the following statements?

   (a) P
   (b) $P \wedge Q$
   (c) $P \vee Q$
3. Suppose that P and Q are statements for which $P \rightarrow Q$ is false. What conclusion (if any) can be made about the truth value of each of the following statements?

   (a) $\urcorner P \rightarrow Q$

(b) $Q \to P$
(c) $P\ veeQ$

4. Suppose that P and Q are statements for which Q is false and $\urcorner P \to Q$ is true (and it is not known if R is true or false). What conclusion (if any) can be made about the truth value of each of the following statements?

   (a) $\urcorner Q \to P$
   (b) P
   (c) $P \wedge R$
   (d) $R \to \urcorner P$
5. Construct a truth table for each of the following statements:

   (a) $P \to Q$
   (b) $Q \to P$
   (c) $\urcorner P \to \urcorner Q$
   (d) $\urcorner Q \to \urcorner P$

   Do any of these statements have the same truth table?
6. Construct a truth table for each of the following statements:

   (a) $P \vee \urcorner Q$
   (b) $\urcorner (P \vee Q)$
   (c) $\urcorner P \vee \urcorner Q$
   (d) $\urcorner P \wedge \urcorner Q$

   Do any of these statements have the same truth table?
7. Construct truth table for $P \wedge (Q \vee R)$ and $(P \wedge Q) \vee (P \wedge R)$. What do you observe.
8. Suppose each of the following statements is true.
   - Laura is in the seventh grade.
   - ��Laura got an A on the mathematics test or Sarah got an A on the mathematics test.
   - ��If Sarah got an A on the mathematics test, then Laura is not in the seventh grade.

     If possible, determine the truth value of each of the following statements. Carefully explain your reasoning.

     (a) Laura got an A on the mathematics test.
     (b) Sarah got an A on the mathematics test.
     (c) Either Laura or Sarah did not get an A on the mathematics test.
9. Let P stand for “the integer x is even,” and let Q stand for “x^2 is even.” Express the conditional statement $P \to Q$ in English using

   (a) The "if then" form of the conditional statement
   (b) The word "Implies"
   (c) The "only if" form of the conditional statement
   (d) The phrase "is necessary for"
   (e) The phrase "is sufficient for"
10. Repeat Exercise (9) for the conditional statement $Q \to P$.
11. For statements P and Q, use truth tables to determine if each of the following statements is a tautology, a contradiction, or neither.
    (a) $\urcorner Q \vee (P \to Q)$.
    (b) $Q \wedge (P \wedge \urcorner Q)$.
    (c) $(Q \wedge P) \wedge (P \to \urcorner Q)$.
    (d) $\urcorner Q \to (P \wedge \urcorner P)$.

12. For statements P, Q, and R:
    (a) Show that $[(P \to Q) \wedge P] \to Q$ is a tautology. **Note**: In symbolic logic, this is an important logical argument form called **modus ponens**.
    (b) Show that $[(P \to Q) \wedge (Q \to R)] \to (P \to R)$ is atautology. **Note**: In symbolic logic, this is an important logical argument form called **syllogism**.

Explorations and Activities

13. **Working with Conditional Statements.** Complete the following table:

English Form	Hypothesis	Conclusion	Symbolic Form
If P, then Q	P	Q	$P \to Q$
Q only if P	Q	P	$Q \to P$
P is necessary for Q			
P is sufficient for Q			
Q is necessary for P			
P implies Q			
P only if Q			
P if Q			
if Q then P			
if $\neg Q$ then $\neg P$			
if Q, then $Q \wedge R$			
if $P \vee Q$, then R			

14. **Working with Truth Values of Statements.** Suppose that P and Q are true statements, that U and V are false statements, and that W is a statement and it is not known if W is true or false.

    Which of the following statements are true, which are false, and for which statements is it not possible to determine if it is true or false? Justify your conclusions.

    (a) $(P \vee Q) \vee (U \wedge W)$ (f) $(\neg P \vee \neg U) \wedge (Q \vee \neg V)$
    (b) $P \wedge (Q \to W)$ (g) $(P \wedge \neg Q) \wedge (U \vee W)$
    (c) $P \wedge (W \to Q)$ (h) $(P \vee \neg Q) \to (U \wedge W)$
    (d) $W \to (P \wedge U)$ (i) $(P \vee W) \to (U \wedge W)$
    (e) $W \to (P \wedge \neg U)$ (j) $(U \wedge \neg V) \to (P \wedge W)$

Answer

Add texts here. Do not delete this text first.

This page titled 2.1: Statements and Logical Operators is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

2.2: Logically Equivalent Statements

Preview Activity 2.2.1: Logically Equivalent Statements

In Exercises (5) and (6) from Section 2.1, we observed situations where two different statements have the same truth tables. Basically, this means these statements are equivalent, and we make the following definition:

Definition

Two expressions are **logically equivalent** provided that they have the same truth value for all possible combinations of truth values for all variables appearing in the two expressions. In this case, we write $X \equiv Y$ and say that X and Y are logically equivalent.

1. Complete truth tables for $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$.
2. Are the expressions $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ logically equivalent?
3. Suppose that the statement “I will play golf and I will mow the lawn” is false. Then its negation is true. Write the negation of this statement in the form of a disjunction. Does this make sense?

   Sometimes we actually use logical reasoning in our everyday living! Perhaps you can imagine a parent making the following two statements:

   Statement 1. If you do not clean your room, then you cannot watch TV.
   Statement 2. You clean your room or you cannot watch TV.
4. Let P be “you do not clean your room,” and let Q be “you cannot watch TV.” Use these to translate Statement 1 and Statement 2 into symbolic forms.
5. Construct a truth table for each of the expressions you determined in Part(4). Are the expressions logically equivalent?
6. Assume that Statement 1 and Statement 2 are false. In this case, what is the truth value of P and what is the truth value of Q? Now, write a true statement in symbolic form that is a conjunction and involves P and Q.
7. Write a truth table for the (conjunction) statement in Part (6) and compare it to a truth table for $\neg(P \to Q)$. What do you observe?

Preview Activity 2.2.2: Converse and Contrapositive

We now define two important conditional statements that are associated with a given conditional statement.

Definition

If P and Q are statements, then

- The **converse** of the conditional statement $P \to Q$ is the conditional statement $Q \to P$.
- The **contrapositive** of the conditional statement $P \to Q$ is the conditional statement $\neg Q \to \neg P$.

1. For the following, the variable x represents a real number. Label each of the following statements as true or false.
   (a) If $x = 3$, then $x^2 = 9$.
   (b) If $x^2 = 9$, then $x = 3$.
   (c) If $x^2 \neq 9$, then $x \neq 3$.
   (d) If $x \neq 3$, then $x^2 \neq 9$.
2. Which statement in the list of conditional statements in Part (1) is the converse of Statement (1a)? Which is the contrapositive of Statement (1a)?
3. Complete appropriate truth tables to show that
   $P \to Q$ is logically equivalent to its contrapositive $\neg Q \to \neg P$.
   $P \to Q$ is not logically equivalent to its converse $Q \to P$

In Preview Activity 2.2.1, we introduced the concept of logically equivalent expressions and the notation $X \equiv Y$ to indicate that statements X and Y are logically equivalent. The following theorem gives two important logical equivalencies. They are sometimes referred to as **De Morgan's Laws**.

Theorem 2.5: De Morgan's Laws

For statements P and Q,

- The statement $\neg(P \wedge Q)$ is logically equivalent to $\neg P \vee \neg Q$. This can be written as $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$.
- The statement $\neg(P \vee Q)$ is logically equivalent to $\neg P \wedge \neg Q$. This can be written as $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$.

Proof

The first equivalency in Theorem 2.5 was established in Preview Activity 2.2.1. Table 2.3 establishes the second equivalency.

Table 2.3: Truth Table for One of De Morgan's Laws

P	Q	$P \vee Q$	$\neg(P \vee Q)$	$\neg P$	$\neg Q$	$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

It is possible to develop and state several different logical equivalencies at this time. However, we will restrict ourselves to what are considered to be some of the most important ones. Since many mathematical statements are written in the form of conditional statements, logical equivalencies related to conditional statements are quite important.

Logical Equivalencies Related to Conditional Statements

The first two logical equivalencies in the following theorem were established in Preview Activity 2.2.1, and the third logical equivalency was established in Preview Activity 2.2.2.

Theorem 2.6

For statements P and Q,

1. The conditional statement $P \to Q$ is logically equivalent to $\neg P \vee Q$.
2. The statement $\neg(P \to Q)$ is logically equivalent to $P \wedge \neg Q$.
3. The conditional statement $P \to Q$ is logically equivalent to its contrapositive $\neg Q \to \neg P$.

The Negation of a Conditional Statement

The logical equivalency $\neg(P \to Q) \equiv P \wedge \neg Q$ is interesting because it shows us that **the negation of a conditional statement is not another conditional statement**. The negation of a conditional statement can be written in the form of a conjunction. So what does it mean to say that the conditional statement

If you do not clean your room, then you cannot watch TV,

is false? To answer this, we can use the logical equivalency $\neg(P \to Q) \equiv P \wedge \neg Q$. The idea is that if $P \to Q$ is false, then its negation must be true. So the negation of this can be written as

You do not clean your room and you can watch TV.

For another example, consider the following conditional statement:

If $-5 < -3$, then $(-5)^2 < (-3)^2$.

This conditional statement is false since its hypothesis is true and its conclusion is false. Consequently, its negation must be true. Its negation is not a conditional statement. The negation can be written in the form of a conjunction by using the logical equivalency $\urcorner(P \to Q) \equiv P \wedge \urcorner Q$. So, the negation can be written as follows:

$$5 < 3 \text{ and } \urcorner((-5)^2 < (-3)^2).$$

However, the second part of this conjunction can be written in a simpler manner by noting that "not less than" means the same thing as "greater than or equal to." So we use this to write the negation of the original conditional statement as follows:

$$5 < 3 \text{ and } (-5)^2 \geq (-3)^2.$$

This conjunction is true since each of the individual statements in the conjunction is true.

Another Method of Establishing Logical Equivalencies

We have seen that it often possible to use a truth table to establish a logical equivalency. However, it is also possible to prove a logical equivalency using a sequence of previously established logical equivalencies. For example,

- $P \to Q$ is logically equivalent to $\urcorner P \vee Q$. So
- $\urcorner(P \to Q)$ is logically equivalent to $\urcorner(\urcorner P \vee Q)$.
- Hence, by one of De Morgan's Laws (Theorem 2.5), $\urcorner(P \to Q)$ is logically equivalent to $\urcorner(\urcorner P) \wedge \urcorner Q$.
- This means that $\urcorner(P \to Q)$ is logically equivalent to$P \wedge \urcorner Q$.

The last step used the fact that $\urcorner(\urcorner P)$ is logically equivalent to P.

When proving theorems in mathematics, it is often important to be able to decide if two expressions are logically equivalent. Sometimes when we are attempting to prove a theorem, we may be unsuccessful in developing a proof for the original statement of the theorem. However, in some cases, it is possible to prove an equivalent statement. Knowing that the statements are equivalent tells us that if we prove one, then we have also proven the other. In fact, once we know the truth value of a statement, then we know the truth value of any other logically equivalent statement. This is illustrated in Progress Check 2.7.

Progress Check 2.7 (Working with a logical equivalency)

In Section 2.1, we constructed a truth table for $(P \wedge \urcorner Q) \to R$.

1. Although it is possible to use truth tables to show that $P \to (Q \vee R)$ is logically equivalent to $P \wedge \urcorner Q) \to R$, we instead use previously proven logical equivalencies to prove this logical equivalency. In this case, it may be easier to start working with $P \wedge \urcorner Q) \to R$. Start with

   $P \wedge \urcorner Q) \to R \equiv \urcorner(P \wedge \urcorner Q) \vee R$,

   which is justified by the logical equivalency established in Part (5) of Preview Activity 1. Continue by using one of De Morgan's Laws on $\urcorner(P \wedge \urcorner Q)$.
2. Let a and b be integers. Suppose we are trying to prove the following:

   If 3 is a factor of $a \cdot b$, then 3 is a factor of a or 3 is a factor of b.

   Explain why we will have proven this statement if we prove the following:

   If 3 is a factor of $a \cdot b$ and 3 is not a factor of a, then 3 is a factor of b.

Answer

Add texts here. Do not delete this text first.

As we will see, it is often difficult to construct a direct proof for a conditional statement of the form $P \to (Q \vee R)$. The logical equivalency in Progress Check 2.7 gives us another way to attempt to prove a statement of the form $P \to (Q \vee R)$. The advantage of the equivalent form, $P \wedge \urcorner Q) \to R$, is that we have an additional assumption, $\urcorner Q$, in the hypothesis. This gives us more information with which to work.

Theorem 2.8 states some of the most frequently used logical equivalencies used when writing mathematical proofs.

Theorem 2.8: important logical equivalencies

For statement P, Q, and R,

De Morgan's Laws $\urcorner(P \wedge Q) \equiv \urcorner P \vee \urcorner Q$.
$\urcorner(P \vee Q) \equiv \urcorner P \wedge \urcorner Q$.

Conditional Statement. $P \to Q \equiv \urcorner Q \to \urcorner P$ (contrapositive)
$P \to Q \equiv \urcorner P \vee Q$
$\urcorner(P \to Q) \equiv P \wedge \urcorner Q$

Biconditional Statement $(Pleftrightarrow Q) \equiv (P \to Q) \wedge (Q \to P)$

Double Negation $\urcorner(\urcorner P) \equiv P$

Distributive Laws $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

Conditionals withDisjunctions $P \to (Q \vee R) \equiv (P \wedge \urcorner Q) \to R$
$(P \vee Q) \to R \equiv (P \to R) \wedge (Q \to R)$

We have already established many of these equivalencies. Others will be established in the exercises.

Exercises for Section 2.2

1. Write the converse and contrapositive of each of the following conditional statements.
    (a) If $a = 5$, then $a^2 = 25$.
    (b) If it is not raining, then Laura is playing golf.
    (c) If $a \neq b$, then $a^4 \neq b^4$.
    (d) If a is an odd integer, then $3a$ is an odd integer.
2. Write each of the conditional statements in Exercise (1) as a logically equiva- lent disjunction, and write the negation of each of the conditional statements in Exercise (1) as a conjunction.
3. Write a useful negation of each of the following statements. Do not leave a negation as a prefix of a statement. For example, we would write the negation of “I will play golf and I will mow the lawn” as “I will not play golf or I will not mow the lawn.”
    (a) We will win the first game and we will win the second game.
    (b) They will lose the first game or they will lose the second game.
    (c) If you mow the lawn, then I will pay you $20.
    (d) If we do not win the first game, then we will not play a second game.
    (e) I will wash the car or I will mow the lawn.
    (f) If you graduate from college, then you will get a job or you will go to graduate school.
    (g) If I play tennis, then I will wash the car or I will do the dishes.
    (h) If you clean your room or do the dishes, then you can go to see a movie.
    (i) It is warm outside and if it does not rain, then I will play golf.
4. Use truth tables to establish each of the following logical equivalencies dealing with biconditional statements:
    (a) $(P \leftrightarrow Q) \equiv (P \to Q) \wedge (Q \to P)$
    (b) $(P \leftrightarrow Q) \equiv (Q \leftrightarrow P)$
    (c) $(P \leftrightarrow Q) \equiv (\urcorner P \leftrightarrow \urcorner Q)$
5. Use truth tables to prove each of the **distributive laws** from Theorem 2.8.

    (a) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
    (b $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

6. Use truth tables to prove the following logical equivalency from Theorem 2.8:

   $[(P \vee Q) \rightarrow R] \equiv (P \rightarrow R) \wedge (Q \rightarrow R)$.
7. Use previously proven logical equivalencies to prove each of the following logical equivalencies about **conditionals with conjunctions:**

   (a) $[(P \wedge Q) \rightarrow R] \equiv (P \rightarrow R) \vee (Q \rightarrow R)$
   (b) $[P \rightarrow (Q \wedge R)] \equiv (P \rightarrow R) \wedge (P \rightarrow R)$
8. If P and Q are statements, is the statement $(P \vee Q) \wedge \neg(P \wedge Q)$ logically equivalent to the statement $(P \wedge \neg Q) \vee (Q \wedge \neg P)$? Justify your conclusion.
9. Use previously proven logical equivalencies to prove each of the following logical equivalencies: (a) $[\neg P \rightarrow (Q \wedge \neg Q)] \equiv P$
   (b) $(P \leftrightarrow Q) \equiv (\neg P \vee Q) \wedge (\neg Q \vee p)$
   (c) $\neg(P \leftrightarrow Q) \equiv (P \wedge \neg Q) \vee (Q \wedge \neg P)$
   (d) $(P \rightarrow Q) \rightarrow R \equiv (P \wedge \neg Q) \vee R$
   (e) $(P \rightarrow Q) \rightarrow R \equiv (\neg P \rightarrow R) \wedge (Q \rightarrow R)$
   (f) $[(P \wedge Q) \rightarrow (R \vee S)] \equiv [(\neg R \wedge \neg S) \rightarrow (\neg P \vee \neg Q)]$
   (g) $[(P \wedge Q) \rightarrow (R \vee S)] \equiv [(P \wedge Q \wedge \neg R) \rightarrow S]$
   (h) $[(P \wedge Q) \rightarrow (R \vee S)] \equiv (\neg P \vee \neg Q \vee R \vee S)$
   (i) $\neg[(P \wedge Q) \rightarrow (R \vee S)] \equiv (P \wedge Q \wedge \neg R \wedge \neg S)$
10. Let a be a real number and let f be a real-valued function defined on an interval containing $x = a$. Consider the following conditional statement:

    If f is differentiable at $x = a$, then f is continuous at $x = a$.

    Which of the following statements have the same meaning as this conditional statement and which ones are negations of this conditional statement?

    Note: This is not asking which statements are true and which are false. It is asking which statements are logically equivalent to the given statement. It might be helpful to let P represent the hypothesis of the given statement, Q represent the conclusion, and then determine a symbolic representation for each statement. Instead of using truth tables, try to use already established logical equivalencies to justify your conclusions.

    (a) If f is continuous at $x = a$, then f is differentiable at $x = a$.
    (b) If f is not differentiable at $x = a$, then f is not continuous at $x = a$.
    (c) If f is not continuous at $x = a$, then f is not differentiable at $x = a$.
    (d) f is not differentiable at $x = a$ or f is continuous at $x = a$.
    (e) f is not continuous at $x = a$ or f is differentiable at $x = a$.
    (f) f is differentiable at $x = a$ or f is not continuous at $x = a$.
11. Let a, b, and c be integers. Consider the following conditional statement:

    If a divides bc, then a divides b or a divides c.

    Which of the following statements have the same meaning as this conditional statement and which ones are negations of this conditional statement?

    The note for Exercise (10) also applies to this exercise.

    (a) If a divides b or a divides c, then a divides bc.
    (b) If a does not divide b or a does not divide c, then a does not divide bc.
    (c) a divides bc, a does not divide b, and a does not divide c.
    (d) If a does not divide b and a does not divide c, then a does not divide bc.
    (e) a does not divide bc or a divides b or a divides c.
    (f) If a divides bc and a does not divide c, then a divides b.
    (g) If a divides bc or a does not divide b, then a divides c.

12. Let x be a real number. Consider the following conditional statement:

    If $x^3 - x = 2x^2 + 6$, then $x = -2$ or $x = 3$.

    Which of the following statements have the same meaning as this conditional statement and which ones are negations of this conditional statement? Explain each conclusion. (See the note in the instructions for Exercise (10).)

    (a) If $x \neq -2$ and $x \neq 3$, then $x^3 - x \neq 2x^2 + 6$.
    (b) If $x = -2$ or $x = 3$, then $x^3 - x = 2x^2 + 6$.
    (c) If $x \neq -2$ or $x \neq 3$, then $x^3 - x \neq 2x^2 + 6$.
    (d) If $x^3 - x = 2x^2 + 6$ and $x \neq -2$, then $x = 3$.
    (e) If $x^3 - x = 2x^2 + 6$ or $x \neq -2$, then $x = 3$.
    (f) $x^3 - x = 2x^2 + 6$, $x \neq -2$, and $x \neq 3$.
    (g) $x^3 - x \neq 2x^2 + 6$ or $x = -2$ or $x = 3$.

    Explorations and Activities

13. **Working with a Logical Equivalency.** Suppose we are trying to prove the following for integers x and y:

    If $x \cdot y$ is even, then x is even or y is even.

    We notice that we can write this statement in the following symbolic form:

    $P \to (Q \vee R)$,

    where P is"$x \cdot y$ is even," Q is"x is even,"and R is "y is even."

    (a) Write the symbolic form of the contrapositive of $P \to (Q \vee R)$. Then use one of De Morgan's Laws (Theorem 2.5) to rewrite the hypothesis of this conditional statement.
    (b) Use the result from Part (13a) to explain why the given statement is logically equivalent to the following statement:

    If x is odd and y is odd, then $x \cdot y$ is odd.

    The two statements in this activity are logically equivalent. We now have the choice of proving either of these statements. If we prove one, we prove the other, or if we show one is false, the other is also false. The second statement is Theorem 1.8, which was proven in Section 1.2.

Answer

Add texts here. Do not delete this text first.

This page titled 2.2: Logically Equivalent Statements is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

2.3: Open Sentences and Sets

? Preview Activity 2.3.1: Sets and Set Notation

The theory of sets is fundamental to mathematics in the sense that many areas of mathematics use set theory and its language and notation. This language and notation must be understood if we are to communicate effectively in mathematics. At this point, we will give a very brief introduction to some of the terminology used in set theory.

A **set** is a well-defined collection of objects that can be thought of as a single entity itself. For example, we can think of the set of integers that are greater than 4. Even though we cannot write down all the integers that are in this set, it is still a perfectly well-defined set. This means that if we are given a specific integer, we can tell whether or not it is in the set of all even integers.

The most basic way of specifying the elements of a set is to list the elements of that set. This works well when the set contains only a small number of objects. The usual practice is to list these elements between braces. For example, if the set C consists of the integer solutions of the equation $x^2 = 9$, we would write

$$C = \{-3, 3\}.$$

For larger sets, it is sometimes inconvenient to list all of the elements of the set. In this case, we often list several of them and then write a series of three dots (...) to indicate that the pattern continues. For example,

$$D = \{1, 3, 5, 7, ... 49\}$$

is the set of all odd natural numbers from 1 to 49, inclusive.

For some sets, it is not possible to list all of the elements of a set; we then list several of the elements in the set and again use a series of three dots (...) to indicate that the pattern continues. For example, if F is the set of all even natural numbers, we could write

$$F = \{2, 4, 6, ...\}.$$

We can also use the three dots before listing specific elements to indicate the pattern prior to those elements. For example, if E is the set of all even integers, we could write

$$E = \{... -6, -4, -2, 0, 2, 4, 6, ...\}.$$

Listing the elements of a set inside braces is called the **roster method** of specifying the elements of the set. We will learn other ways of specifying the elements of a set later in this section.

1. Use the roster method to specify the elements of each of the following sets:

   (a) The set of real numbers that are solutions of the equation $x^2 - 5x = 0$.
   (b) The set of natural numbers that are less than or equal to 10.
   (c) The set of integers that are greater than -2.
2. Each of the following sets is defined using the roster method. For each set, determine four elements of the set other than the ones listed using the roster method.
   $A = \{1, 4, 7, 10, ...\}$
   $B = \{2, 4, 8, 16, ...\}$
   $C = \{..., -8, -6, -4, -2, 0\}$
   $D = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$

? Preview Activity 2.3.2: Variables

Not all mathematical sentences are statements. For example, an equation such as

$$x^2 - 5 = 0$$

is not a statement. In this sentence, the symbol x is a **variable**. It represents a number that may be chosen from some specified set of numbers. The sentence (equation) becomes true or false when a specific number is substituted for x.

1. (a) Does the equation $x^2 - 25 = 0$ become a true statement if -5 is substituted for x?
   (b) Does the equation $x^2 - 25 = 0$ become a true statement if $\sqrt{5}$ is substituted for x?

Definition

A **variable** is a symbol representing an unspecified object that can be chosen from a given set U. The set U is called the **universal set for the variable**. It is the set of specified objects from which objects may be chosen to substitute for the variable. A **constant** is a specific member of the universal set.

Some sets that we will use frequently are the usual number systems. Recall that we use the symbol $\mathbb{R}$ to stand for the set of all **real numbers**, the symbol $\mathbb{Q}$ to stand for the set of all **rational numbers**, the symbol $\mathbb{Z}$ to stand for the set of all **integers**, and the symbol $\mathbb{N}$ to stand for the set of all **natural numbers**.

A **variable** is a symbol representing an unspecified object that can be chosen from some specified set of objects. This specified set of objects is agreed to in advance and is frequently called the **universal set**.

2. What real numbers will make the sentence “$y^2 - 2y - 15 = 0$” a true statement when substituted for y?
3. What natural numbers will make the sentence “$y^2 - 2y - 15 = 0$” a true statement when substituted for y?
4. What real numbers will make the sentence "$\sqrt{x}$ is a real number" a true statement when substituted for x?
5. What real numbers will make the sentence "$sin^2 x + cos^2 x = 1$" a true statement when substituted for x?
6. What natural numbers will make the sentence "$\sqrt{n}$ is a natural number" a true statement when substituted for n?
7. What real numbers will make the sentence

   $\int_0^y t^2 dt > 9$

   a true statement when substituted for y?

Some Set Notation

In Preview Activity $2.3.1$, we indicated that a set is a well-defined collection of objects that can be thought of as an entity itself.

- If $A$is a set and y is one of the objects in the set A, we write $y \in A$ and read this as “y is an element of A” or “y is a member of A.” For example, if B is the set of all integers greater than 4, then we could write $5 \in B$ and $10 \in B$.
- If an object z is not an element in the set A, we write $z \notin A$ and read this as “z is not an element of A.” For example, if B is the set of all integers greater than 4, then we could write $2 \notin B$ and $4 \notin B$.

When working with a mathematical object, such as set, we need to define when two of these objects are equal. We are also often interested in whether or not one set is contained in another set.

Definitions: Equal sets and Subsets

Two sets, A and B, are *equal* when they have precisely the same elements. In this case, we write $A = B$. When the sets A and B are not equal, we write $A \notin B$.

The set A is a *subset* of a set B provided that each element of A is an element of B. In this case, we write $A \subseteq B$ and also say that A is *contained* in B. When A is not a subset of B, we write $A \nsubseteq B$.

Using these definitions, we see that for any set A, $A = A$ and since it is true that for each $x \in U$, if $x \in A$, then $x \in A$, we also see that $A \subseteq A$. That is, any set is equal to itself and any set is a subset of itself. For some specific examples, we see that:

- {1, 3, 5} = {3, 5, 1}
- {5, 10} = {5, 10, 5}
- {4, 8, 12} = {4, 4, 8, 12, 12}
- {5, 10} $\neq$ {5, 10, 15} but {5,10} $\subseteq$ {5, 10, 15} and {5, 10, 15} $\nsubseteq$ {5, 10}.

In each of the first three examples, the two sets have exactly the same elements even though the elements may be repeated or written in a different order.

? Progress Check 2.9 (Set Notation)

1. Let A = {-4, -2, 0, 2, 4, 6, 8, ...}. Use correct set notation to indicate which of the following integers are in the set A and which are not in the set A. For example, we could write 6 $\in A$ and 5 $\notin A$.

   10 22 13 -3 0 -12
2. Use correct set notation (using = or $\subseteq$) to indicate which of the following sets are equal and which are subsets of one of the other sets.

   A = {3, 6, 9}. B = {6, 9, 3, 6}
   C = {3, 6, 9, ... } D = {3, 6, 7, 9}
   E = {9, 12, 15, ... } F = {9, 7, 6, 2}

Answer

Add texts here. Do not delete this text first.

Variables and Open Sentences

As we have seen in the Preview Activities, not all mathematical sentences are statements. This is often true if the sentence contains a variable. The following terminology is useful in working with sentences and statements.

Definition: Open Sentence

An **open sentence** is a sentence $P(x_1, x_2, ..., x_n)$ involving variables $x_1, x_2, ..., x_n$ with the property that when specific values from the universal set are assigned to $x_1, x_2, ..., x_n$, then the resulting sentence is either true or false. That is, the resulting sentence is a statement. An open sentence is also called a **predicate** or a **propositional function**.

Notation: One reason an open sentence is sometimes called a *propositional function* is the fact that we use function notation $P(x_1, x_2, ..., x_n)$ for an open sentence in n variables. When there is only one variable, such as x, we write $P(X)$, which is read "P of x." In this notation, x represents an arbitrary element of the universal set, and $P(x)$ represents a sentence. When we substitute a specific element of the universal set for x, the resulting sentence becomes a statement. This is illustrated in the next example.

✓ Example 2.10: Open Sentences

If the universal set is $\mathbb{R}$, then the sentence "$x^2 - 3x - 10 = 0$" is an open sentence involving the one variable x.

- If we substitute $x = 2$, we obtain the false statement "$2^2 - 3 \cdot 2 - 10 = 0$."
- If we substitute $x = 5$, we obtain the true statement "$5^2 - 3 \cdot 5 - 10 = 0$."

In this example, we can let $P(x)$ be the predicate "$x^2 - 3x - 10 = 0$" and then say that $P(2)$ is false and $P(5)$ is true.

Using similar notation, we can let $Q(x, y)$ be the predicate "$x + 2y = 7$." This predicate involves two variables. Then,

- $Q(1, 1)$ is false since "$1 + 2 \cdot 1 = 7$" is false; and
- $Q(3, 2)$ is true since "$3 + 2 \cdot 2 = 7$" is false.

? Progress Check 2.11: Working with Open Sentences

1. Assume the universal set for all variable is $\mathbb{Z}$ and let $P(x)$ be the predicate "$x^2 \leq 4$."
   (a) Find two values of x for which $P(x)$ is false.
   (b) Find two values of x for which $P(x)$ is true.
   (c) Use the roster method to specify the set of all x for which $P(x)$ is true.
2. Assume the universal set for all variable is $\mathbb{Z}$ and let $R(x, y, z)$ be the predicate "$x^2 + y^2 = z^2$."
   (a) Find two different examples for which $R(x, y, z)$ is false.
   (b) Find two different examples for which $R(x, y, z)$ is true.

Answer

Add texts here. Do not delete this text first.

Without using the term, Example 2.10 and Progress Check 2.11 (and Preview Activity $2.3.2$) dealt with a concept called the truth set of a predicate.

Definition: truth set of an open sentence with one variable

The *truth set of an open sentence with one variable* is the collection of objects in the universal set that can be substituted for the variable to make the predicate a true statement.

One part of elementary mathematics consists of learning how to solve equations. In more formal terms, the process of solving an equation is a way to determine the truth set for the equation, which is an open sentence. In this case, we often call the truth set the **solution set**. Following are three examples of truth sets.

- If the universal set is $\mathbb{R}$, then the truth set of the equation $3x-8=10$ is the set {6}.
- If the universal set is $\mathbb{R}$, then the truth set of the equation $x^2-3x-10=0$ is {-2, 5}.
- If the universal set is $\mathbb{N}$, then the truth set of the open sentence "$\sqrt{n}\in\mathbb{N}$" is {1, 4, 9, 16, ...}.

Set Builder Notation

Sometimes it is not possible to list all the elements of a set. For example, if the universal set is $\mathbb{R}$, we cannot list all the elements of the truth set of “$x^2<4$.” In this case, it is sometimes convenient to use the so-called **set builder notation** in which the set is defined by stating a rule that all elements of the set must satisfy. If $P(x)$ is a predicate in the variable x, then the notation

$$\{x\in U|P(x)\}$$

stands for the set of all elements x in the universal set U for which $P(x)$ is true. If it is clear what set is being used for the universal set, this notation is sometimes shortened to $\{x|P(x)\}$. This is usually read as “the set of all x such that $P(x)$.” The vertical bar stands for the phrase “such that.” Some writers will use a colon (:) instead of the vertical bar.

For a non-mathematical example, P could be the property that a college student is a mathematics major. Then $\{x|P(x)\}$ denotes the set of all college students who are mathematics majors. This could be written as

$$\{x\mid x \text{ is a college student who is a mathematics major}\}.$$

Example 2.12 (Truth Sets)

Assume the universal set is $\mathbb{R}$ and $P(x)$ is "$x^2<4$." We can describe the truth set of $P(x)$ as the set of all real numbers whose square is less than 4. We can also use set builder notation to write the truth set of $P(x)$ as

$$\{x\in\mathbb{R}|x^2<4\}$$

However, if we solve the inequality $x^2<4$, we obtain $-2<x<2$. So we could also write the truth set as

$$\{x\in\mathbb{R}|-2<x<4\}$$

We could read this as the set of all real numbers that are greater than -2 and less than 2. We can also write

$$\{x\in\mathbb{R}|x^2<4\}=\{x\in\mathbb{R}|-2<x<4\}$$

Progress Check 2.13 (Working with Truth Sets)

Let $P(x)$ be the predicate "$x^2\le 9$."

1. If the universal set is $\mathbb{R}$, describe the truth set of $P(x)$ using English and write the truth set of $P(x)$ using set builder notation.
2. If the universal set is $\mathbb{Z}$, then what is the truth set of $P(x)$? Describe this set using English and then use the roster method to specify all the elements of this truth set.
3. Are the truth sets in Parts (1) and (2) equal? Explain.

Answer

Add texts here. Do not delete this text first.

So far, our standard form for set builder notation has been $\{x \in U | P(x)\}$. It is sometimes possible to modify this form and put the predicate first. For example, the set

$$\{A = 3n + 1 | n \in \mathbb{N}\}$$

describes the set of all natural numbers of the form $3n + 1$ for some natural number.

By substituting 1, 2, 3, 4, and so on, for n, we can use the roster method to write

$$A = \{3n + 1 | n \in \mathbb{N}\} = \{4, 7, 10, 13, ... \}.$$

We can sometimes “reverse this process” by starting with a set specified by the roster method and then writing the same set using set builder notation.

✓ Example 2.14 (Set Builder Notation)

Let B = {..., -11. -7, -3, 1, 5, 9, 13, ...}. The key to writing this set using set builder notation is to recognize the pattern involved. We see that once we have an integer in B, we can obtain another integer in B by adding 4. This suggests that the predicate we will use will involve multiplying by 4.

Since it is usually easier to work with positive numbers, we notice that $1 \in B$ and $5 \in B$. Notice that

$$1 = 4 \cdot 0 + 1 \text{ and } 5 = 4 \cdot 1 + 1.$$

This suggests that we might try $4n + 1 | n \in z$. In fact, by trying other integers for n, we can see that

$$B = \{..., -11, -7, -3, 1, 5, 9, 13, ...\} = \{4n + 1 | n \in \mathbb{Z}\}.$$

? Progress Check 2.15 (Set Builder Notation)

Each of the following sets is defined using the roster method.

A = {1, 5, 9, 13, ...} C = { $\sqrt{2}$, $(\sqrt{2})^3$, $(\sqrt{2})^5$, ... }

B = {..., -8, -6, -4, -2, 0} D = {1, 3, 9, 27, ...}

1. Determine four elements of each set other than the ones listed using the roster method.
2. Use set builder notation to describe each set.

Answer

Add texts here. Do not delete this text first.

The Empty Set

When a set contains no elements, we say that the set is the empty set. For example, the set of all rational numbers that are solutions of the equation $x^2 = -$��2 is the empty set since this equation has no solutions that are rational numbers.

In mathematics, the empty set is usually designated by the symbol $\emptyset$. We usually read the symbol $\emptyset$ as “the empty set” or “the null set.” (The symbol $\emptyset$ is actually the last letter in the Danish-Norwegian alphabet.)

When the Truth Set Is the Universal Set

The truth set of a predicate can be the universal set. For example, if the universal set is the set of real numbers $\mathbb{R}$, then the truth set of the predicate “$x + 0 = x$” is $\mathbb{R}$.

Notice that the sentence “$x + 0 = x$” has not been quantified and a particular element of the universal set has not been substituted for the variable x. Even though the truth set for this sentence is the universal set, we will adopt the convention that unless the quantifier is stated explicitly, we will consider the sentence to be a predicate or open sentence. So, with this convention, if the universal set is $\mathbb{R}$, then

- $x + 0 = x$ is a predicate;

- For each real number x, $x + 0 = x$ is a statement.

Exercises for Section 2.3

1. Use the roster method to specify the elements in each of the following sets and then write a sentence in English describing the set.
   (a) $\{x \in \mathbb{R} | 2x^2 + 3x - 2 = 0\}$
   (b) $\{x \in \mathbb{Z} | 2x^2 + 3x - 2 = 0\}$
   (c) $\{x \in \mathbb{Z} | x^2 < 25\}$
   (d) $\{x \in \mathbb{N} | x^2 < 25\}$
   (e) $\{y \in \mathbb{Q} | |y - 2| = 2.5\}$
   (f) $\{y \in \mathbb{Z} | |y - 2| \leq 2.5\}$
2. Each of the following sets is defined using the roster method.

   A= {1, 4, 9, 16, 25, ...}
   B = {..., -π^4, -π^3, -π^2, -π, 0...}
   C = {3, 9, 15, 21, 27, ...}
   D = {0, 4, 8, ..., 96, 100}

   (a) Determine four elements of each set other than the ones listed using the roster method.
   (b) Use set builder notation to describe each set.
3. Let A = $\{x \in \mathbb{R} | x(x+2)^2(x - \frac{3}{2} = 0\}$. Which of the following sets are equal to the set A and which are subsets of A?

   (a) $\{-2, 0, 3\}$
   (b) $\{-2, -2, 0, \frac{3}{2}\}$
   (c) $\{\frac{3}{2}, -2, 0\}$
   (d) $\{-2, \frac{3}{2}\}$
4. Use the roster method to specify the truth set for each of the following open sentences. The universal set for each open sentence is the set of integers $\mathbb{Z}$.

   (a) $n + 7 = 4$.
   (b) $n^2 = 64$.
   (c) $\sqrt{n} \in \mathbb{N}$ and n is less than 50.
   (d) n is an odd integer that is greater than 2 and less than 14.
   (e) n is an even integer that is greater than 10.
5. Use set builder notation to specify the following sets:

   (a) The set of all integers greater than or equal to 5.
   (b) The set of all even integers.
   (c) The set of all positive rational numbers.
   (d) The set of all real numbers greater than 1 and less than 7.
   (e) The set of all real numbers whose square is greater than 10.
6. For each of the following sets, use English to describe the set and when appropriate, use the roster method to specify all of the elements of the set.

   (a) $\{x \in \mathbb{R} | -3 \leq x \leq 5\}$
   (b) $\{x \in \mathbb{Z} | -3 \leq x \leq 5\}$
   (c) $\{x \in \mathbb{R} | x^2 = 16\}$
   (d) $\{x \in \mathbb{R} | x^2 + 16 = 0\}$
   (e) $\{x \in \mathbb{Z} | x$ is odd$\}$
   (f) $\{x \in \mathbb{R} | 3x - 4 \geq 17\}$

Explorations and Activities

7. **Closure Explorations**. In Section 1.1, we studied some of the closure properties of the standard number systems. (See page 10.) We can extend this idea to other sets of numbers. So we say that:

- A set A of numbers is **closed under addition** provided that whenever x and y are are in the set A, $x+y$ is in the set A.
- A set A of numbers is **closed under multiplication** provided that whenever x and y are are in the set A, $x \cdot y$ is in the set A.
- A set A of numbers is **closed under subtraction** provided that whenever x and y are are in the set A, $x-y$ is in the set A.

For each of the following sets, make a conjecture about whether or not it is closed under addition and whether or not it is closed under multiplication. In some cases, you may be able to find a counterexample that will prove the set is not closed under one of these operations.
(a) The set of all odd natural numbers
(b) The set of all even integers
(c) A = {1, 4, 7, 10, 13, ...}
(d) B = {..., -6, -3, 0, 3, 6, 9, ...}
(e) C = $\{3n+1 | n \in \mathbb{Z}\}$
(f) D = $\{\frac{1}{2^n} | n \in \mathbb{N}\}$

Answer

Add texts here. Do not delete this text first.

This page titled 2.3: Open Sentences and Sets is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

2.4: Quantifiers and Negations

Preview Activity 1 (An Introduction to Quantifiers)

We have seen that one way to create a statement from an open sentence is to substitute a specific element from the universal set for each variable in the open sentence. Another way is to make some claim about the truth set of the open sentence. This is often done by using a quantifier. For example, if the universal set is $\mathbb{R}$, then the following sentence is a statement.

For each real number x, $x^2 > 0$.

The phrase “For each real number x” is said to **quantify the variable** that follows it in the sense that the sentence is claiming that something is true for all real numbers. So this sentence is a statement (which happens to be false).

Definition: universal quantifier

The phrase “for every” (or its equivalents) is called a *universal quantifier*. The phrase “there exists” (or its equivalents) is called an **existential quantifier**. The symbol $\forall$ is used to denote a universal quantifier, and the symbol $\exists$ is used to denote an existential quantifier.

Using this notation, the statement “For each real number x, $x^2 > 0$” could be written in symbolic form as: $(\forall x \in \mathbb{R})(x^2 > 0)$. The following is an example of a statement involving an existential quantifier.

There exists an integer x such that $3x - 2 = 0$.

This could be written in symbolic form as

$$(\exists x \in \mathbb{Z})(3x - 2 = 0).$$

This statement is false because there are no integers that are solutions of the linear equation $3x - 2 = 0$. Table 2.4 summarizes the facts about the two types of quantifiers.

A statement involving	Often has the form	The statement is true provided that
A universal quantifier: $(\forall x, P(x))$	"For every x, $P(x)$," where $P(x)$ is a predicate.	Every value of x in the universal set makes $P(x)$ true.
An existential quantifier: $(\exists x, P(x))$	"There exists an x such that $P(x)$," where $P(x)$ is a predicate.	There is at least one value of x in the universal set that makes $P(x)$ true.

Table 2.4: Properties of Quantifiers

In effect, the table indicates that the universally quantified statement is true provided that the truth set of the predicate equals the universal set, and the existentially quantified statement is true provided that the truth set of the predicate contains at least one element.

Each of the following sentences is a statement or an open sentence. Assume that the universal set for each variable in these sentences is the set of all real numbers. If a sentence is an open sentence (predicate), determine its truth set. If a sentence is a statement, determine whether it is true or false.

1. $(\forall a \in \mathbb{R})(a + 0 = a)$.
2. $3x - 5 = 9$.
3. $\sqrt{x} \in \mathbb{R}$.
4. $sin(2x) = 2(sinx)(cosx)$.
5. $(\forall x \in \mathbb{R})(sin(2x) = 2(sinx)(cosx))$.
6. $(\exists x \in \mathbb{R})(x^2 + 1 = 0)$.
7. $(\forall x \in \mathbb{R})(x^3 \geq x^2)$.
8. $x^2 + 1 = 0$.
9. If $x^2 \geq 1$, then $x \geq 1$.
10. $(\forall x \in \mathbb{R})$ (If $x^2 \geq 1$, then $x \geq 1$).

Preview Activity 2 (Attempting to Negate Quantified Statements)

1. Consider the following statement written in symbolic form:
   $(\forall x \in \mathbb{Z})$ (x is a multiple of 2).

   (a) Write this statement as an English sentence.
   (b) Is the statement true or false? Why?
   (c) How would you write the negation of this statement as an English sentence?
   (d) If possible, write your negation of this statement from part(2) symbolically (using a quantifier).
2. Consider the following statement written in symbolic form:
   $(\exists x \in \mathbb{Z})$ $(x^3 > 0)$.

   (a) Write this statement as an English sentence.
   (b) Is the statement true or false? Why?
   (c) How would you write the negation of this statement as an English sentence?
   (d) If possible, write your negation of this statement from part(2) symbolically (using a quantifier).

We introduced the concepts of open sentences and quantifiers in Section 2.3

Forms of Quantified Statements in English

There are many ways to write statements involving quantifiers in English. In some cases, the quantifiers are not apparent, and this often happens with conditional statements. The following examples illustrate these points. Each example contains a quantified statement written in symbolic form followed by several ways to write the statement in English.

1. $(\forall x \in \mathbb{R})$ $(x^2 > 0)$.

   - For each real number x, $x^2 > 0$.
   - The square of every real number is greater than 0.
   - The square of a real number is greater than 0.
   - If $x \in \mathbb{R}$, then $x^2 > 0$.

   In the second to the last example, the quantifier is not stated explicitly. Care must be taken when reading this because it really does say the same thing as the previous examples. The last example illustrates the fact that conditional statements often contain a “hidden” universal quantifier.

   If the universal set is $\mathbb{R}$, then the truth set of the open sentence $x^2 > 0$ is the set of all nonzero real numbers. That is, the truth set is

   $\{x \in \mathbb{R} | x \neq 0\}$

   So the preceding statements are false. For the conditional statement, the example using $x = 0$ produces a true hypothesis and a false conclusion. This is a **counterexample** that shows that the statement with a universal quantifier is false.

2. $(\exists x \in \mathbb{R})$ $(x^2 = 5)$.

   - There exists a real number x such that $x^2 = 5$.
   - $x^2 = 5$ for some real number x.
   - There is a real number whose square equals 5.

   The second example is usually not used since it is not considered good writing practice to start a sentence with a mathematical symbol.
   If the universal set is $\mathbb{R}$, then the truth set of the predicate "$x^2 = 5$" is $\{-sqrt5, sqrt5\}$. So these are all true statements.

Negations of Quantified Statements

In Preview Activity 2.4.1, we wrote negations of some quantified statements. This is a very important mathematical activity. As we will see in future sections, it is sometimes just as important to be able to describe when some object does not satisfy a certain property as it is to describe when the object satisfies the property. Our next task is to learn how to write negations of quantified statements in a useful English form.

We first look at the negation of a statement involving a universal quantifier. The general form for such a statement can be written as $(\forall x \in U)\ (P(x))$, where $P(x)$is an open sentence and U is the universal set for the variable x. When we write

$$\urcorner(\forall x \in U)[P(x)],$$

we are asserting that the statement $\forall x \in U)[P(x)]$ is false. This is equivalent to saying that the truth set of the open sentence $P(x)$ is not the universal set. That is, there exists an element x in the universal set U such that $P(x)$ is false. This in turn means that there exists an element x in U such that $\urcorner P(x)$ is true, which is equivalent to saying that $(\exists x \in U)[\urcorner P(x)]$ is true. This explains why the following result is true:

$$\urcorner(\forall x \in U)[P(x)] \equiv (\exists x \in U)[\urcorner P(x)]$$

Similarly, when we write

$$\urcorner(\exists x \in U)[P(x)]$$

we are asserting that the statement $(\exists x \in U)[P(x)]$ is false. This is equivalent to saying that the truth set of the open sentence $P(x)$ is the empty set. That is, there is no element x in the universal set U such that $P(x)$ is true. This in turn means that for each element x in U, $\urcorner P(x)$ is true, and this is equivalent to saying that $(\forall x \in U)[\urcorner P(x)]$ is true. This explains why the following result is true:

$$\urcorner(\exists x \in U)[P(x)] \equiv (\forall x \in U)[\urcorner P(x)]$$

We summarize these results in the following theorem.

✓ Theorem 2.16.

For any open sentence $P(x)$,

$$\urcorner(\forall x \in U)[P(x)] \equiv (\exists x \in U)[\urcorner P(x)], \text{ and}$$

$$\urcorner(\exists x \in U)[P(x)] \equiv (\forall x \in U)[\urcorner P(x)]$$

✓ Example 2.17 (Negations of Quantified Statements)

Consider the following statement: $(\forall x \in \mathbb{R})(x^3 \geq x^2)$.

We can write this statement as an English sentence in several ways. Following are two different ways to do so.

- For each real number x, $x^3 \geq x^2$.
- If x is a real number, then x^3 is greater than or equal to x^2.

The second statement shows that in a conditional statement, there is often a hidden universal quantifier. This statement is false since there are real numbers x for which x^3 is not greater than or equal to x^2. For example, we could use $x = -1$ or $x = \frac{1}{2}$. This means that the negation must be true. We can form the negation as follows:

$$\urcorner(\forall x \in \mathbb{R})(x^3 \geq x^2) \equiv (\exists x \in \mathbb{R})\urcorner(x^3 \geq x^2).$$

In most cases, we want to write this negation in a way that does not use the negation symbol. In this case, we can now write the open sentence $\urcorner(x^3 \geq x^2)$ as $(x^3 < x^2)$. (That is, the negation of "is greater than or equal to" is "is less than.") So we obtain the following:

$$\urcorner(\forall x \in \mathbb{R})(x^3 \geq x^2) \equiv (\exists x \in \mathbb{R})(x^3 < x^2).$$

The statement $(\exists x \in \mathbb{R})(x^3 < x^2)$ could be written in English as follows:

- There exists a real number x such that $x^3 < x^2$.
- There exists an x such that x is a real number and $x^3 < x^2$.

? Progress Check 2.18 (Negating Quantified Statements)

For each of the following statements

- Write the statement in the form of an English sentence that does not use the symbols for quantifiers.
- Write the negation of the statement in a symbolic form that does not use the negation symbol.
- Write the negation of the statement in the form of an English sentence that does not use the symbols for quantifiers.

1. $(\forall a \in \mathbb{R})(a+0=a)$.
2. $(\forall x \in \mathbb{R})[sin(2x)=2(sinx)(cosx)]$.
3. $(\forall x \in \mathbb{R})(tan^2 x+1=sec^2 x)$.
4. $(\exists x \in \mathbb{Q})(x^2-3x-7=0)$.
5. $(\exists x \in \mathbb{R})(x^2+1=0)$.

Answer

Add texts here. Do not delete this text first.

Counterexamples and Negations of Conditional Statements

The real number $x=-1$ in the previous example was used to show that the statement $(\forall x \in \mathbb{R})(x^3 \geq x^2)$ is false. This is called a **counterexample** to the statement. In general, a **counterexample** to a statement of the form $(\forall x)[P(x)]$ is an object a in the universal set U for which $P(a)$ is false. It is an example that proves that $(\forall x)[P(x)]$ is a false statement, and hence its negation, $(\exists x)[\urcorner P(x)]$, is a true statement.

In the preceding example, we also wrote the universally quantified statement as a conditional statement. The number $x=-1$ is a counterexample for the statement

If x is a real number, then x^3 is greater than or equal to x^2.

So the number -1 is an example that makes the hypothesis of the conditional statement true and the conclusion false. Remember that a conditional statement often contains a “hidden” universal quantifier. Also, recall that in Section 2.2 we saw that the negation of the conditional statement “If P then Q” is the statement “P and not Q.” Symbolically, this can be written as follows:

$$\urcorner(P \rightarrow Q) \equiv P \wedge \urcorner Q.$$

So when we specifically include the universal quantifier, the symbolic form of the negation of a conditional statement is

$$\urcorner(\forall x \in U)[P(x) \rightarrow Q(x)] \equiv (\exists x \in U)\urcorner[P(x) \rightarrow Q(x)] \equiv (\exists x \in U)[P(x) \wedge \urcorner Q(x)].$$

That is,

$$\urcorner(\forall x \in U)[P(x) \rightarrow Q(x)] \equiv (\exists x \in U)[P(x) \wedge \urcorner Q(x)].$$

Progress Check 2.19 (Using Counterexamples)

Use counterexamples to explain why each of the following statements is false.

1. For each integer n, (n^2+n+1) is a prime number.
2. For each real number x, if x is positive, then $2x^2>x$.

Answer

Add texts here. Do not delete this text first.

Quantifiers in Definitions

Definitions of terms in mathematics often involve quantifiers. These definitions are often given in a form that does not use the symbols for quantifiers. Not only is it important to know a definition, it is also important to be able to write a negation of the definition. This will be illustrated with the definition of what it means to say that a natural number is a perfect square.

Definition: perfect square

A natural number n is a *perfect square* provided that there exists a natural number k such that $n=k^2$.

This definition can be written in symbolic form using appropriate quantifiers as follows:

A natural number n is a **perfect square** provided $(\exists k \in \mathbb{N})(n=k^2)$.

We frequently use the following steps to gain a better understanding of a definition.

1. Examples of natural numbers that are perfect squares are 1, 4, 9, and 81 since $1 = 1^2$, $4 = 2^2$, $9 = 3^2$, and $81 = 9^2$.
2. Examples of natural numbers that are not perfect squares are 2, 5, 10, and 50.
3. This definition gives two “conditions.” One is that the natural number n is a perfect square and the other is that there exists a natural number k such that $n = k^2$. The definition states that these mean the same thing. So when we say that a natural number n is not a perfect square, we need to negate the condition that there exists a natural number k such that $n = k^2$. We can use the symbolic form to do this.

$$\urcorner(\exists k \in \mathbb{N})(n = k^2) \equiv (\forall k \in \mathbb{N})(n \neq k^2)$$

Notice that instead of writing $\urcorner(n = k^2)$, we used the equivalent form of $(n \neq k^2)$. This will be easier to translate into an English sentence. So we can write,

> A natural number n is not a perfect square provided taht for every natural number k, $n \neq k^2$.

The preceding method illustrates a good method for trying to understand a new definition. Most textbooks will simply define a concept and leave it to the reader to do the preceding steps. Frequently, it is not sufficient just to read a definition and expect to understand the new term. We must provide examples that satisfy the definition, as well as examples that do not satisfy the definition, and we must be able to write a coherent negation of the definition

? Progress Check 2.20 (Multiples of Three)

Definition

An integer n is a **multiple of 3** provided that there exists an integer k such that $n = 3k$.

1. Write this definition in symbolic form using quantifiers by completing the following:

   An integer n is a multiple of 3 provided that ...
2. Give several examples of integers (including negative integers) that are multiples of 3.
3. Give several examples of integers (including negative integers) that are not multiples of 3.
4. Use the symbolic form of the definition of a multiple of 3 to complete the following sentence: “An integer n is not a multiple of 3 provided that . . . .”
5. Without using the symbols for quantifiers, complete the following sentence: “An integer \(n\0 is not a multiple of 3 provide that . . . .”

Answer

Add texts here. Do not delete this text first.

Statements with More than One Quantifier

When a predicate contains more than one variable, each variable must be quantified to create a statement. For example, assume the universal set is the set of integers, $\mathbb{Z}$, and let $P(x, y)$ be the predicate, “$x + y = 0$.” We can create a statement from this predicate in several ways.

1. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x + y = 0)$.
   We could read this as,“ For all integers x and y, $x + y = 0$.” This is a false statement since it is possible to find two integers whose sum is not zero $2 + 3 \neq 0$.
2. $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x + y = 0)$.
   We could read this as, “For every integer x, there exists an integer y such that $x + y = 0$.” This is a true statement.
3. $(\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x + y = 0)$.
   We could read this as, “There exists an integer x such that for each integer y, $x + y = 0$.” This is a false statement since there is no integer whose sum with each integer is zero.
4. $(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x + y = 0)$.
   We could read this as, “There exist integers x and y such that $x + y = 0$.” This is a true statement. For example, $2 + (-2) = 0$

When we negate a statement with more than one quantifier, we consider each quantifier in turn and apply the appropriate part of Theorem 2.16. As an example, we will negate Statement (3) from the preceding list. The statement is

$$(\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x+y=0).$$

We first treat this as a statement in the following form: $(\exists x \in \mathbb{Z})(P(x))$ where $P(x)$ is the predicate $(\forall y \in \mathbb{Z})(x+y=0)$. Using Theorem 2.16, we have

$$\neg(\exists x \in \mathbb{Z})(P(x)) \equiv (\forall x \in \mathbb{Z})(\neg P(x)).$$

Using Theorem 2.16 again, we obtain the following:

$$\begin{aligned} \neg P(x) &\equiv \neg(\forall y \in \mathbb{Z})(x+y=0) \\ &\equiv (\exists y \in \mathbb{Z})\neg(x+y=0) \\ &\equiv (\exists y \in \mathbb{Z})(x+y \neq 0). \end{aligned}$$

Combining these two results, we obtain

$$\neg(\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x+y=0) \equiv (\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x+y \neq 0).$$

The results are summarized in the following table.

	Symbolic Form	**English Form**
Statement	$(\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x+y=0)$	There exists an integer x such that for each integer y, $x+y=0$.
Negation	$(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x+y \neq 0)$	For each integer x, there exists an integer y such that $x+y \neq 0$.

Since the given statement is false, its negation is true.
We can construct a similar table for each of the four statements. The next table shows Statement (2), which is true, and its negation, which is false.

	Symbolic Form	**English Form**
Statement	$(\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x+y=0)$	For every integer x, there exists an integer y such that $x+y=0$.
Negation	$(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x+y \neq 0)$	There exists an integer x such that for every integer y, $x+y \neq 0$.

? Progress Check 2.21 (Negating a Statement with Two Quantifiers)

Write the negation of the statement

$$(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x+y=0)$$

in symbolic form and as a sentence written in English.

Answer

Add texts here. Do not delete this text first.

Writing Guideline

Try to use English and minimize the use of cumbersome notation. Do not use the special symbols for quantifiers $\forall$ (for all), $\exists$ (there exists), $backepsilon$ (such that), or $\therefore$ (therefore) in formal mathematical writing. It is often easier to write and usually easier to read, if the English words are used instead of the symbols. For example, why make the reader interpret

$$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x+y=0)$$

when it is possible to write

For each real number x, there exists a real number y such that $x+y=0$, or, more succinctly (if appropriate),

Every real number has an additive inverse.

Exercises for Section 2.4

1. For each of the following, write the statement as an English sentence and then explain why the statement is false.

   (a) $(\exists x \in \mathbb{Q})(x^2 - 3x - 7 = 0)$.
   (b) $(\exists x \in \mathbb{R})(x^2 + 1 = 0)$.
   (c) $(\exists m \in \mathbb{N})(m^{<}1)$.
2. For each of the following, use a counterexample to show that the statement is false. Then write the negation of the statement in English, without using symbols for quantifiers.

   (a) $(\forall m \in \mathbb{Z})$ (m^2 is even).
   (b)$(\forall x \in \mathbb{R})(x^2 > 0)$.
   (c) For each real number x, $\sqrt{x} \in \mathbb{R}$.
   (d) $(\forall m \in \mathbb{Z})(\frac{m}{3} \in \mathbb{Z})$.
   (e) $(\forall a \in \mathbb{Z})(\sqrt{a^2} = a)$.
   (f) $(\forall x \in \mathbb{R})(tan^2 x + 1 = sec^2 x)$.
3. For each of the following statements
   - Write the statement as an English sentence that does not use the symbols for quantifiers.
   - Write the negation of the statement in symbolic form in which the negation symbol is not used.
   - Write a useful negation of the statement in an English sentence that does not use the symbols for quantifiers.

   (a) $(\exists x \in \mathbb{Q})(x > \sqrt{2})$.
   (b) $(\forall x \in \mathbb{Q})(x^2 - 2 \neq 0)$.
   (c) $(\forall x \in \mathbb{Z})$ (x is even or x is odd).
   (d) $(\exists x \in \mathbb{Q})(\sqrt{2} < x < \sqrt{3})$. **Note**: The sentence "$\sqrt{2} < x < \sqrt{3}$" is actually a conjunction. It means $\sqrt{2} < x$ and $x < \sqrt{3}$.
   (e) $(\forall x \in \mathbb{Z})$ (If x^2 is odd, then x is odd).
   (f) $(\forall n \in \mathbb{N})$ [If n is a perfect sqare, then $(2^n - 1)$ is not a prime number].
   (g) $(\forall n \in \mathbb{N})$ ($n^2 - n + 41$ is a prime number).
   (h) $(\exists x \in \mathbb{R})(cos(2x) = 2(cos x))$.
4. Write each of the following statements as an English sentence that does not use the symbols for quantifiers.

   (a) $(\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})(m > n)$
   (b) $(\exists m \in \mathbb{Z})(\forall n \in \mathbb{Z})(m > n)$
   (c) $(\forall m \in \mathbb{Z})(\exists n \in \mathbb{Z})(m > n)$
   (d) $(\forall m \in \mathbb{Z})(\forall n \in \mathbb{Z})(m > n)$
   (e) $(\exists m \in \mathbb{Z})(\forall n \in \mathbb{Z})(m^2 > n)$
   (f) $(\forall m \in \mathbb{Z})(\exists n \in \mathbb{Z})(m^2 > n)$
5. Write the negation of each statement in Exercise (4) in symbolic form and as an English sentence that does not use the symbols for quantifiers.
6. Assume that the universal set is $\mathbb{Z}$. Consider the following sentence:

   $(\exists t \in \mathbb{Z})(t \cdot x = 20)$.

   (a) Explain why this sentence is an open sentence and not a statement.
   (b) If 5 is substituted for x, is the resulting sentence a statement? If it is a statement, is the statement true or false?
   (c) If 8 is substituted for x, is the resulting sentence a statement? If it is a statement, is the statement true or false?
   (d) If 2 is substituted for x, is the resulting sentence a statement? If it is a statement, is the statement true or false?
   (e) What is the truth set of the open sentence $(\exists t \in \mathbb{Z})(t \cdot x = 20)$?
7. Assume that the universal set is $\mathbb{R}$. Consider the following sentence:

   $(\exists t \in \mathbb{R})(t \cdot x = 20)$.

(a) Explain why this sentence is an open sentence and not a statement.
(b) If 5 is substituted for x, is the resulting sentence a statement? If it is a statement, is the statement true or false?
(c) If π is substituted for x, is the resulting sentence a statement? If it is a statement, is the statement true or false?
(d) If 0 is substituted for x, is the resulting sentence a statement? If it is a statement, is the statement true or false?
(e) What is the truth set of the open sentence $(\exists t \in \mathbb{R})(t \cdot x = 20)$?

8. Let $\mathbb{Z}^*$ be the set of all nonzero integers.

   (a) Use a counterexample to explain why the following statement is false:
   For each $x \in \mathbb{Z}^*$, there exists a $y \in \mathbb{Z}^*$ such that $xy = 1$.
   (b) Write the statement in part(a) in symbolic form using appropriate symbols for quantifiers.
   (c) Write the negation of the statement in part (b) in symbolic form using appropriate symbols for quantifiers.
   (d) Write the negation from part(c) in English without usings the symbols for quantifiers.

9. An integer m is said to have the *divides property* provided that for all integers a and b, if m divides ab, then m divides a or m divides b.

   (a) Using the symbols for quantifiers, write what it means to say that the integer m has the divides property.
   (b) Using the symbols for quantifiers, write what it means to say that the integer m does not have the divides property.
   (c) Write an English sentence stating what it means to say that the integer m does not have the divides property.

10. In calculus, we define a function f with domain $\mathbb{R}$ to be **strictly increasing** provided that for all real numbers x and y, $f(x) < f(y)$ whenever $x < y$. Complete each of the following sentences using the appropriate symbols for quantifiers:
    (a) A function f with domain $\mathbb{R}$ is strictly increasing provided that ...
    (b) A function f with domain $\mathbb{R}$ is not strictly increasing provided that ...

    Complete the following sentence in English without using symbols for quantifiers:

    (c) A function f with domain $\mathbb{R}$ is not strictly increasing provided that ...

11. In calculus, we define a function f to be **continuous** at a real number a provided that for every $\varepsilon > 0$, there exists a $\delta > 0$ such that if $|x - a| < \delta$, then $|f(x) - f(a)| < \varepsilon$.

    Note: The symbol ε is the lowercase Greek letter epsilon, and the symbol δ is the lowercase Greek letter delta.

    Complete each of the following sentences using the appropriate symbols for quantifiers:

    (a) A function f is continuous at the real number a provided that ...
    (b) A function f is not continuous at the real number a provided that ...

    Complete the following sentence in English without using symbols for quantifiers:

    (c) A function f is not continuous at the real number a provided that ...

12. The following exercises contain definitions or results from more advanced mathematics courses. Even though we may not understand all of the terms involved, it is still possible to recognize the structure of the given statements and write a meaningful negation of that statement.

    (a) In abstract algebra, an operation $*$ on a set A is called a **commutative operation** provided that for all $x, y \in A$, $x * y = y * x$. Carefully explain what it means to say that an operation $*$ on a set A is not a commutative operation.

    (b) In abstract algebra, a **ring** consists of a nonempty set R and two operations called addition and multiplication. A nonzero element a in a ring R is called a zero divisor provided that there exists a nonzero element b in R such that $ab = 0$. Carefully explain what it means to say that a nonzero element a in a ring R is not a zero divisor.

    (c) A set M of real numbers is called a **neighborhood** of a real number aprovided that there exists a positive real number ϵ such that the open interval $(a - \epsilon, a + \epsilon)$ is contained in M. Carefully explain what it means to say that a set M is not a neighborhood of a real number a.

(d) In advanced calculus, a sequence of real numbers $\{x_1, x_2, ..., x_k, ...\}$ is called a **Cauchy sequence** provided that for each positive real number, there exists a natural number N such that for all $m; n \in \mathbb{N}$, if $m > N$ and $n > N$, then $|x_n - x_m| < \epsilon$. Carefully explain what it means to say that the sequence of real numbers $\{x_1, x_2, ..., x_k, ...\}$ is not a Cauchy sequence.

Explorations and Activities

13. **Prime Numbers.** The following definition of a prime number is very important in many areas of mathematics. We will use this definition at various places in the text. It is introduced now as an example of how to work with a definition in mathematics.

Definition

A natural number p is a **prime number** provided that it is greater than 1 and the only natural numbers that are factors of p are 1 and p. A natural number other than 1 that is not a prime number is a **composite number**. The number 1 is neither prime nor composite.

Using the definition of a prime number, we see that 2, 3, 5, and 7 are prime numbers. Also, 4 is a composite number since 4 = 2 $\cdot$ 2; 10 is a composite number since 10 = 2 $\cdot$ 5; and 60 is a composite number since 60 = 4 $\cdot$ 15.

(a) Give examples of four natural numbers other than 2, 3, 5, and 7 that are prime numbers.
(b) Explain why a natural number p that is greater than 1 is a prime number provided that
For all $d \in \mathbb{N}$, if d is a factor of p, then $d = 1$ or $d = p$.
(c) Give examples of four natural numbers that are composite numbers and explain why they are composite numbers.
(d) Write a useful description of what it means to say that a natural number is a composite number (other than saying that it is not prime).

14. **Upper Bounds for Subsets of** $\mathbb{R}$. Let A be a subset of the real numbers. A number b is called an **upper bound** for the set A provided that for each element x in A, $x \le b$.

(a) Write this definition in symbolic form by completing the following:
Let A be a subset of the real numbers. A number b is called an upper bound for the set A provided that ...
(b) Give examples of three different upper bounds for the set $A = \{x \in \mathbb{R} | 1 \le x \le 3\}$.
(c) Does the set $B = \{x \in \mathbb{R} | x > 0\}$ have an upper bound? Explain.
(d) Give examples of three different real numbers that are not upper bounds for the set $A = \{x \in \mathbb{R} | 1 \le x \le 3\}$.
(e) Complete the following in symbolic form: “Let A be a subset of $\mathbb{R}$. A number b is not an upper bound for the set A provided that ...”
(f) Without using the symbols for quantifiers, complete the following sentence: “Let A be a subset of $\mathbb{R}$. A number b is not an upper bound for the set A provided that ...”
(g) Are your examples in Part(14d) consistent with your work in Part(14f)? Explain.

15. **Least Upper Bound for a Subset of** $\mathbb{R}$. In Exercise 14, we introduced the definition of an upper bound for a subset of the real numbers. Assume that we know this definition and that we know what it means to say that a number is not an upper bound for a subset of the real numbers.

Let A be a subset of $\mathbb{R}$. A real number is the **least upper bound** for A provided that α is an upper bound for A, and if β is an upper bound for A, then $\alpha \le \beta$.

Note: The symbol α is the lowercase Greek letter alpha, and the symbol β is the lowercase Greek letter beta.

If we define $P(x)$ to be “x is an upper bound for A,” then we can write the definition for least upper bound as follows:

A real number is the **least upper bound** for A provided that
$P(\alpha) \wedge [(\forall \beta \in \mathbb{R})(P(\beta) \rightarrow (\alpha \le \beta))]$.

(a) Why is a universal quantifier used for the real number β?
(b) Complete the following sentence in symbolic form: “A real number α is not the least upper bound for A provided that ...

(c) Complete the following sentence as an English sentence: "A real number α is not the least upper bound for A provided that ..."

Answer

Add texts here. Do not delete this text first.

This page titled 2.4: Quantifiers and Negations is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

2.S: Logical Reasoning (Summary)

Important Definitions

- Logically equivalent statements, page 43
- Converse of a conditional statement, page 44
- Contrapositive of a conditional statement, page 44
- Equal sets, page 55
- Variable, page 54
- Universal set for a variable, page 54
- Constant, page 54
- Predicate, page 54
- Open sentence, page 54
- Truth set of a predicate, page 58
- Universal quantifier, page 63
- Existential quantifier, page 63
- Empty set, page 60
- Counterexample, page 66 and 69
- Perfect square, page 70
- Prime number, page 78
- Composite number, page 78

Important Theorems and Results

Theorem 2.8. Important Logical Equivalencies. *For statements* P, Q, *and* R,

De Morgan's Laws $\urcorner(P \wedge Q) \equiv \urcorner P \vee \urcorner Q$
$\urcorner(P \vee Q) \equiv \urcorner P \wedge \urcorner Q$

Conditional Statement $P \to Q \equiv \urcorner Q \to \urcorner P$ (contrapostitive)
$P \to Q \equiv \urcorner P \vee Q$
$\urcorner(P \to Q) \equiv P \wedge \urcorner Q$

Biconditional Statement $(P \leftrightarrow Q) \equiv (P \to Q) \wedge (Q \to P)$

Double Negation $\urcorner(\urcorner P) \equiv P$

Distributive Laws $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

Conditionals with Disjunctions $P \to (Q \vee R) \equiv (P \wedge \urcorner Q) \to R$
$P \vee Q) \to R \equiv (P \to R) \wedge (Q \to R)$

Theorem 2.16. Negations of Quantified Statements. *For any predicate* $P(x)$,

$$\urcorner(\forall x)[P(x)] \equiv (\exists x)[\urcorner P(x)], \text{ and}$$
$$\urcorner(\exists x)[P(x)] \equiv (\forall x)[\urcorner P(x)]$$

Important Set Theory Notation

Notation	Description	Page
$y \in A$	y is an element of the set A.	55
$z \notin A$	z is not an element of the set A.	55
{ }	The roster method	53
$\{x \in U \vert P(x)\}$	Set builder notation	58

This page titled 2.S: Logical Reasoning (Summary) is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

CHAPTER OVERVIEW

3: Constructing and Writing Proofs in Mathematics

A *proof* in mathematics is a convincing argument that some mathematical statement is true. A proof should contain enough mathematical detail to be convincing to the person(s) to whom the proof is addressed. In essence, a proof is an argument that communicates a mathematical truth to another person (who has the appropriate mathematical background). A proof must use correct, logical reasoning and be based on previously established results. These previous results can be axioms, definitions, or previously proven theorems. These terms are discussed in the sections below.

3.1: Direct Proofs
3.2: More Methods of Proof
3.3: Proof by Contradiction
3.4: Using Cases in Proofs
3.5: The Division Algorithm and Congruence
3.6: Review of Proof Methods
3.S: Constructing and Writing Proofs in Mathematics (Summary)

This page titled 3: Constructing and Writing Proofs in Mathematics is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

3.1: Direct Proofs

Preview Activity 1 (Definition of Divides, Divisor, Multiple)
In Section 1.2, we studied the concepts of even integers and odd integers. The definition of an even integer was a formalization of our concept of an even integer as being one this is "divisible by 2," or a "multiple of 2." We could also say that if "2 divides an integer," then that integer is an even integer. We will now extend this idea to integers other than 2. Following is a formal definition of what it means to say that a nonzero integer m divides an integer n.

> **Definition**
>
> A nonzero integer m **divides** an integer n provided that there is an integer q such that $n = m \cdot q$. We also say that m is a **divisor** of n, m is a **factor** of n, and n is a **multiple** of m. The integer 0 is not a divisor of any integer. If a and b are integers and $a \neq 0$, we frequently use the notation $a \mid b$as a shorthand for "a divides b."

A Note about Notation: Be careful with the notation $a \mid b$. This does not represent the rational number $\frac{a}{b}$. The notation $a \mid b$ represents a relationship between the integers a and b and is simply a shorthand for "a divides b."

A Note about Definitions: Technically, a definition in mathematics should almost always be written using "if and only if." It is not clear why, but the convention in mathematics is to replace the phrase "if and only if" with "if" or an equivalent. Perhaps this is a bit of laziness or the "if and only if" phrase can be a bit cumbersome. In this text, we will often use the phrase "provided that" instead.

The definition for "divides" can be written in symbolic form using appropriate quantifiers as follows: A nonzero integer m **divides** an integer n provided that $(\exists q \in \mathbb{Z})(n = m \cdot q)$.

1. Use the definition of divides to explain why 4 divides 32 and to explain why 8 divides -96.
2. Give several examples of two integers where the first integer does not divide the second integer.
3. According to the definition of "divides," does the integer 10 divide the integer 0? That is, is 10 a divisor of 0? Explain.
4. Use the definition of "divides" to complete the following sentence in symbolic form: "The nonzero integer m does not divide the integer n means that ...."
5. Use the definition of "divides" to complete the following sentence without using the symbols for quantifiers: "The nonzero integer m does not divide the integer n. ...."
6. Give three different examples of three integers where the first integer divides the second integer and the second integer divides the third integer.

   As we have seen in Section 1.2, a definition is frequently used when constructing and writing mathematical proofs. Consider the following conjecture:

   > **Conjecture:** Let a, b and c be integers with $a \neq 0$ and $b \neq 0$. If a divides b and b divides c, then a divides c.

7. Explain why the examples you generated in part (6) provide evidence that this conjecture is true.

   In Section 1.2, we also learned how to use a **know-show table** to help organize our thoughts when trying to construct a proof of a statement. If necessary, review the appropriate material in Section 1.2.

8. State precisely what we would assume if we were trying to write a proof of the preceding conjecture.
9. Use the definition of "divides" to make some conclusions based on your assumptions in part (8).
10. State precisely what we would be trying to prove if we were trying to write a proof of the conjecture.
11. Use the definition of divides to write an answer to the question, "How can we prove what we stated in part (10)?

Preview Activity 2 (Calendars and Clocks)
This preview activity is intended to help with understanding the concept of congruence, which will be studied at the end of this section.

1. Suppose that it is currently Tuesday. (a) What day will it be 3 days from now?
   (b) What day will it be 10 days from now?
   (c) What day will it be 17 days from now? What day will it be 24 days from now?
   (d) Find several other natural numbers x such that it will be Friday x days from now.

   (e) Create a list (in increasing order) of the numbers 3; 10; 17; 24, and the numbers you generated in Part (1d). Pick any two numbers from this list and subtract one from the other. Repeat this several times.
   (f) What do the numbers you obtained in Part (1e) have in common?
2. Suppose that we are using a twelve-hour clock with no distinction between A.M. and P.M. Also, suppose that the current time is 5:00. (a) What time will it be 4 hours from now?
   (b) What time will it be 16 hours from now? What time will it be 28 hours from now?
   (c) Find several other natural numbers x such that it will be 9:00 x hours from now.
   (d) Create a list (in increasing order) of the numbers 4; 16; 28, and the numbers you generated in Part (2c). Pick any two numbers from this list and subtract one from the other. Repeat this several times.
   (e) What do the numbers you obtained in Part (2d) have in common?
3. This is a continuation of Part (1). Suppose that it is currently Tuesday.

   (a) What day was it 4 days ago?
   (b) What day was it 11 days ago? What day was it 18 days ago?
   (c) Find several other natural numbers x such that it was Friday x days ago.
   (d) Create a list (in increasing order) consisting of the numbers18; 11; 4, the opposites of the numbers you generated in Part (3c) and the positive numbers in the list from Part (1e). Pick any two num- bers from this list and subtract one from the other. Repeat this several times.
   (e) What do the numbers you obtained in Part (3d) have in common?

Some Mathematical Terminology

In Section 1.2, we introduced the idea of a direct proof. Since then, we have used some common terminology in mathematics without much explanation. Before we proceed further, we will discuss some frequently used mathematical terms.

A **proof** in mathematics is a convincing argument that some mathematical statement is true. A proof should contain enough mathematical detail to be convincing to the person(s) to whom the proof is addressed. In essence, a proof is an argument that communicates a mathematical truth to another person (who has the appropriate mathematical background). A proof must use correct, logical reasoning and be based on previously established results. These previous results can be axioms, definitions, or previously proven theorems. These terms are discussed below.

Surprising to some is the fact that in mathematics, there are always **undefined terms**. This is because if we tried to define everything, we would end up going in circles. Simply put, we must start somewhere. For example, in Euclidean geometry, the terms "point," "line," and "contains" are undefined terms. In this text, we are using our number systems such as the natural numbers and integers as undefined terms. We often assume that these undefined objects satisfy certain properties. These assumed relationships are accepted as true without proof and are called axioms (or postulates). An **axiom** is a mathematical statement that is accepted without proof. Euclidean geometry starts with undefined terms and a set of postulates and axioms. For example, the following statement is an axiom of Euclidean geometry:

Given any two distinct points, there is exactly one line that contains these two points.

> The closure properties of the number systems discussed in Section 1.1 and the properties of the number systems in Table 1.2 on page 18 are being used as axioms in this text.

A **definition** is simply an agreement as to the meaning of a particular term. For example, in this text, we have defined the terms "even integer" and "odd integer." Definitions are not made at random, but rather, a definition is usually made because a certain property is observed to occur frequently. As a result, it becomes convenient to give this property its own special name. Definitions that have been made can be used in developing mathematical proofs. In fact, most proofs require the use of some definitions.

In dealing with mathematical statements, we frequently use the terms "conjecture," "theorem," "proposition," "lemma," and "corollary." A **conjecture** is a statement that we believe is plausible. That is, we think it is true, but we have not yet developed a proof that it is true. A **theorem** is a mathematical statement for which we have a proof. A term that is often considered to be synonymous with "theorem" is proposition.

Often the proof of a theorem can be quite long. In this case, it is often easier to communicate the proof in smaller "pieces." These supporting pieces are often called lemmas. A **lemma** is a true mathematical statement that was proven mainly to help in the proof of some theorem. Once a given theorem has been proven, it is often the case that other propositions follow immediately from the fact that the theorem is true. These are called corollaries of the theorem. The term **corollary** is used to refer to a theorem that is easily proven once some other theorem has been proven.

Constructing Mathematical Proofs

To create a proof of a theorem, we must use correct logical reasoning and mathematical statements that we already accept as true. These statements include axioms, definitions, theorems, lemmas, and corollaries.

In Section 1.2, we introduced the use of a **know-show table** to help us organize our work when we are attempting to prove a statement. We also introduced some guidelines for writing mathematical proofs once we have created the proof. These guidelines should be reviewed before proceeding.

Please remember that when we start the process of writing a proof, we are essentially “reporting the news.” That is, we have already discovered the proof, and now we need to report it. This reporting often does not describe the process of discovering the news (the investigative portion of the process).

Quite often, the first step is to develop a conjecture. This is often done after working within certain objects for some time. This is what we did in Preview Activity $3.1.1$ when we used examples to provide evidence that the following conjecture is true:

> **Conjecture:** Let a, b and c be integers with $a \neq 0$ and $b \neq 0$. If a divides b and b divides c, then a devides c.

Before we try to prove a conjecture, we should make sure we have explored some examples. This simply means to construct some specific examples where the integers a, b, and c satisfy the hypothesis of the conjecture in order to see if they also satisfy the conclusion. We did this for this conjecture in Preview Activity $3.1.1$.

We will now start a know-show table for this conjecture.

Step	**Know**	**Reason**
P	$a, b, c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, $a \mid b$ and $b \mid c$	Hypothesis
$P1$		
...	...	...
$Q1$		
Q	$a \mid c$	
Step	**Show**	**Reason**

The backward question we ask is, “How can we prove that a divides c?” One answer is to use the definition and show that there exists an integer q such that $c = a \cdot q$. This could be step $Q1$ in the know-show table.

We now have to prove that a certain integer q exists, so we ask the question, “How do we prove that this integer exists?” When we are at such a stage in the backward process of a proof, we usually turn to what is known in order to prove that the object exists or to find or construct the object we are trying to prove exists. We often say that we try to “construct” the object or at least prove it exists from the known information. So at this point, we go to the forward part of the proof to try to prove that there exists an integer q such that $c = a \cdot q$.

The forward question we ask is, “What can we conclude from the facts that $a \mid b$ and $b \mid c$?” Again, using the definition, we know that there exist integers s and t such that $b = a \cdot s$ and $c = b \cdot t$. This could be step $P1$ in the know-show table.

The key now is to determine how to get from $P1$ to $Q1$. That is, can we use the conclusions that the integers s and t exist in order to prove that the integer q (from the backward process) exists. Using the equation $b = a \cdot s$, we can substitute $a \cdot s$ for b in the second equation, $c = b \cdot t$. This gives

$$\begin{aligned} c &= b \cdot t \\ &= (a \cdot s) \cdot t \\ &= a(s \cdot t). \end{aligned}$$

The last step used the associative property of multiplication. (See Table 1.2 on page 18.) This shows that c is equal to a times some integer. (This is because $s \cdot t$ is an integer by the closure property for integers.) So although we did not use the letter q, we have arrived at step $Q1$. The completed know-show table follows.

Step	Know	Reason
P	a, b, $c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, $a \mid b$ and $b \mid c$	Hypothesis
$P1$	$(\exists s \in \mathbb{Z})(b = a \cdot s)$ $(\exists t \in \mathbb{Z})(c = b \cdot t)$	Definition of "Divides"
$P2$	$c = (a \cdot s) \cdot t$	Substitution for b
$P3$	$c = a \cdot (s \cdot t)$	Associative property of multiplication
$Q1$	$(\exists q \in \mathbb{Z})(c = a \cdot q)$	Step $P3$ and the closure properties of the integers
Q	$a \mid c$	Definition of "divides"

Notice the similarities between what we did for this proof and many of the proofs about even and odd integers we constructed in Section 1.2. When we try to prove that a certain object exists, we often use what is called the **construction method for a proof**. The appearance of an existential quantifier in the show (or backward) portion of the proof is usually the indicator to go to what is known in order to prove the object exists.

We can now report the news by writing a formal proof.

Theorem 3.1

Let a, b and c be integers with $a \neq 0$ and $b \neq 0$. If a divides b and b divides c, then a divides c.

Proof

We assume that a, b, and c are integers with $a \neq 0$ and $b \neq 0$. We further assume that a divides b and that b divides c. We will prove that a divides c.

Since a divides b and b divides c, there exist an integers s and t such that

$$b = a \cdot s, and \tag{3.1.1}$$

$$c = b \cdot t \tag{3.1.2}$$

We can now substitute the expression for b from equation (1) into equation (2). This gives

$$c = (a \cdot s) \cdot t.$$

Using the associate property for multiplication, we can rearrange the right side of the last equation to obtain

$$c = a \cdot (s \cdot t).$$

Because both s and t are integers, and since the integers are closed under multiplication, we know that $s \cdot t \in \mathbb{Z}$. Therefore, the previous equation proves that a divides c. Consequently, we have proven that whenever a, b, and c are integers with $a \neq 0$ and $b \neq 0$ such that a divides b and b divides c, then a divides c.

Writing Guidelines for Equation Numbers

We wrote the proof for Theorem 3.1 according to the guidelines introduced in Section 1.2, but a new element that appeared in this proof was the use of equation numbers. Following are some guidelines that can be used for **equation numbers**.

If it is necessary to refer to an equation later in a proof, that equation should be centered and displayed. It should then be given it a number. The number for the equation should be written in parentheses on the same line as the equation at the right-hand margin as in shown in the following example.

Since x is an odd integer, there exists an integer n such that

$$x = 2n + 1 \tag{3.1.3}$$

.

Later in the proof, there may be a line such as

Then, using the result in equation (1), we obtain . . . .

Notice that we did not number every equation in Theorem 3.1. We should only number those equations we will be referring to later in the proof, and we should only number equations when it is necessary. For example, instead of numbering an equation, it is often better to use a phrase such as, “the previous equation proves that . . . ” or “we can rearrange the terms on the right side of the previous equation.” Also, note that the word “equation” is not capitalized when we are referring to an equation by number. Although it may be appropriate to use a capital “E,” the usual convention in mathematics is not to capitalize.

? Progress Check 3.2 (A Property of Divisors)

1. Give at least four different examples of integers a, b, and c with $a \neq 0$ such that a divides b and a divides c.
2. For each example in Part (1), calculate the sum $b + c$. Does the integer a divide the sum $b + c$?
3. Construct a know-show table for the following proposition: For all integers a, b, and c with $a \neq 0$, if a divides b and a divides c, then a divides $b + c$.

Answer

Add texts here. Do not delete this text first.

Using Counterexamples

In Section 1.2 and so far in this section, our focus has been on proving statements that involve universal quantifiers. However, another important skill for mathematicians is to be able to recognize when a statement is false and then to be able to prove that it is false. For example, suppose we want to know if the following proposition is true or false.

For each integer n, if 5 divides $n^2 - 1$, then 5 divides $n - 1$.

Suppose we start trying to prove this proposition. In the backward process, we would say that in order to prove that 5 divides $n - 1$, we can show that there exists an integer k such that

$$Q_1 : n - 1 = 5k \text{ or } n = 5k + 1.$$

For the forward process, we could say that since 5 divides (n^2 - 1), we know that there exists an interger m such that

$$P_1 \colon n^2 - 1 = 5m \text{ or } n^2 = 5m + 1.$$

The problem is that there is no straightforward way to use P_1 to prove Q_1. At this point, it would be a good idea to try some examples for n and try to find situations in which the hypothesis of the proposition is true. (In fact, this should have been done before we started trying to prove the proposition.) The following table summarizes the results of some of these explorations with values for n.

n	$n^2 - 1$	Does 5 divide $(n^2 - 1)$	$n - 1$	Does 5 divide $(n - 1)$
1	0	yes	0	yes
2	3	no	1	no
3	8	no	2	no
4	15	yes	3	no

We can stop exploring examples now since the last row in the table provides an example where the hypothesis is true and the conclusion is false. Recall from Section 2.4 (see page 69) that a **counterexample** for a statement of the form $\forall x \in U)(P(x))$ is an element a in the universal set for which $P(a)$ is false. So we have actually proved that the negation of the proposition is true.

When using a counterexample to prove a statement is false, we do not use the term “proof” since we reserve a proof for proving a proposition is true. We could summarize our work as follows:

Conjecture. For each integer n, if 5 divides (n^2 - 1), then 5 divides (n - 1).

The integer n = 4 is a counterexample that proves this conjecture is false. Notice that when n = 4, n^2 - 1 = 15 and 5 divides 15. Hence,the hypothesis of the conjecture is true in this case. In addition, n - 1 = 3 and 5 does not divide 3 and so the conclusion of the conjecture is false in this case. Since this is an example where the hypothesis is true and the conclusion is false, the conjecture is false.

As a general rule of thumb, anytime we are trying to decide if a proposition is true or false, it is a good idea to try some examples first. The examples that are chosen should be ones in which the hypothesis of the proposition is true. If one of these examples makes the conclusion false, then we have found a counterexample and we know the proposition is false. If all of the examples produce a true conclusion, then we have evidence that the proposition is true and can try to write a proof.

? Progress Check 3.3: Using a Counterexample

Use a counterexample to prove the following statement is false.

For all integers a and b, if 5 divides a or 5 divides b, then 5 divides (5a + b).

Answer

Add texts here. Do not delete this text first.

Congruence

What mathematicians call congruence is a concept used to describe cycles in the world of the integers. For example, the day of the week is a cyclic phenomenon in that the day of the week repeats every seven days. The time of the day is a cyclic phenomenon because it repeats every 12 hours if we use a 12-hour clock or every 24 hours if we use a 24-hour clock. We explored these two cyclic phenomena in Preview Activity 3.1.2.

Similar to what we saw in Preview Activity 3.1.2, if it is currently Monday, then it will be Wednesday 2 days from now, 9 days from now, 16 days from now, 23 days from now, and so on. In addition, it was Wednesday 5 days ago, 12 days ago, 19 days ago, and so on. Using negative numbers for time in the past, we generate the following list of numbers:

..., -19, -12, -5, 2, 9, 16, 23, ...

Notice that if we subtract any number in the list above from any other number in that list, we will obtain a multiple of 7. For example,

✓ Example:

$$16 - 2 = 14 = 7 \cdot 2$$

$$(-5) - (9) = -14 = 7 \cdot (-2)$$

$$16 - (-12) = 28 = 7 \cdot 4.$$

Using the concept of congruence, we would say that all the numbers in this list are congruent modulo 7, but we first have to define when two numbers are congruent modulo some natural number n.

Definition

Let $n \in \mathbb{N}$. If a and b are integers, then we say that a **is congruent to** b **modulo** n provided that n divides $a - b$. A standard notation for this is $a \equiv b \pmod{n}$. This is read as "a is congruent to b modulo n" or "a is congruent to b mod n."

Notice that we can use the definition of divides to say that n divides $a - b$ if and only if there exists an integer k such that $a - b = nk$. So we can write

$$a \equiv b \pmod{n} \text{ means } (\exists k \in \mathbb{Z})(a - b = nk), \text{ or}$$
$$a \equiv b \pmod{n} \text{ means } (\exists k \in \mathbb{Z})(a = b + nk).$$

This means that in order to find integers that are congruent to b modulo n, we only need to add multiples of n to b. For example, to find integers that are congruent to 2 modulo 5, we add multiples of 5 to 2. This gives the following list:

... -13, -8, -3, 2, 7, 12, 17,...

We can also write this using set notation and say that

$$\{a \in \mathbb{Z} | a \equiv 2 \text{ (mod 5)}\} = \{\ldots -13, -8, -3, 2, 7, 12, 17, \ldots\}$$

? Progress Check 3.4 (Congruence Modulo 8)

1. Determine at least eight different integers that are congruent to 5 modulo 8.
2. Usesetbuildernotationandtherostermethodtospecifythesetofallintegers

   that are congruent to 5 modulo 8.
3. Choose two integers that are congruent to 5 modulo 8 and add them. Then repeat this for at least five other pairs of integers that are congruent to 5 modulo 8.
4. Explain why all of the sums that were obtained in Part (3) are congruent to 2 modulo 8.

Answer

Add texts here. Do not delete this text first.

We will study the concept of congruence modulo n in much more detail later in the text. For now, we will work with the definition of congruence modulo n in the context of proofs. For example, all of the examples used in Progress Check 3.4should provide evidence that the following proposition is true.

Proposition 3.5.

For all integers a and b, if $a \equiv 5$ (mod 8) and $b \equiv 5$ (mod 8), then $(a + b) \equiv 2$ (mod 8).

? Progress Check 3.6 (Proving Proposition 3.5)

We will use “backward questions” and “forward questions” to help construct a proof for Proposition 3.5. So, we might ask, “How do we prove that $(a + b) \equiv 2$ (mod 8)” One way to answer this is to use the definition of congruence and state that$(a + b)$ $\equiv$ 2 (mod 8) provided that 8 divides $(a + b - 2)$.

1. Use the definition of divides to determine a way to prove that 8 divides $(a + b - 2)$.

   We now turn to what we know and ask, "What can we conclude from the assumptions that $a \equiv 5$ (mod 8) and $b \equiv 5$ (mod 8)." We can again use the definition of congruence and conclude that 8 divides (a - 5) and 8 divides (b - 5).
2. Use the definition of divides to make conclusions based on the facts that 8 divides (a - 5) and 8 divides (b - 5).
3. Solve an equation from part (2) for a and for b.
4. Use the results from part (3) to prove that 8 divides $(a + b - 2)$.
5. Write a proof for Proposition 3.5.

Answer

Add texts here. Do not delete this text first.

Additional Writing Guidelines

We will now be writing many proofs, and it is important to make sure we write according to accepted guidelines so that our proofs may be understood by others. Some writing guidelines were introduced in Chapter 1. The first four writing guidelines given below can be considered general guidelines, and the last three can be considered as technical guidelines specific to writing in mathematics.

1. **Know your audience**. Every writer should have a clear idea of the intended audience for a piece of writing. In that way, the writer can give the right amount of information at the proper level of sophistication to communicate effectively. This is

especially true for mathematical writing. For example, if a mathematician is writing a solution to a textbook problem for a solutions manual for instructors, the writing would be brief with many details omitted. However, if the writing was for a students' solution manual, more details would be included.

2. **Use complete sentences and proper paragraph structure.** Good grammar is an important part of any writing. Therefore, conform to the accepted rules of grammar. Pay careful attention to the structure of sentences. Write proofs using **complete sentences** but avoid run-on sentences. Also, do not forget punctuation, and always use a spell checker when using a word processor.
3. **Keep it simple.** It is often difficult to understand a mathematical argument no matter how well it is written. Do not let your writing help make it more difficult for the reader. Use simple, declarative sentences and short paragraphs, each with a simple point.
4. **Write a first draft of your proof and then revise it**. Remember that a proof is written so that readers are able to read and understand the reasoning in the proof. Be clear and concise. Include details but do not ramble. Do not be satisfied with the first draft of a proof. Read it over and refine it. Just like any worthwhile activity, learning to write mathematics well takes practice and hard work. This can be frustrating. Everyone can be sure that there will be some proofs that are difficult to construct, but remember that proofs are a very important part of mathematics. So work hard and have fun.
5. **Do not use $*$ for multiplication or ˆ for exponents.** Leave this type of notation for writing computer code. The use of this notation makes it difficult for humans to read. In addition, avoid using / for division when using a complex fraction.

   For example, it is very difficult to read $(x^3 - 3x^2 + 1/2)/(2x/3 - 7)$; the fraction

   $$\frac{x^3 - 3x^2 + \dfrac{1}{2}}{\dfrac{2x}{3} - 7} \tag{3.1.4}$$

   is much easier to read.
6. **Do not use a mathematical symbol at the beginning of a sentence.** For example, we should not write, "Let n be an integer. n is an odd integer provided that . . . ." Many people find this hard to read and often have to re- read it to understand it. It would be better to write, "An integer n is an odd integer provided that . . . ."
7. **Use English and minimize the use of cumbersome notation.** Do not use the special symbols for quantifiers ∀ (for all), $exists$ (there exists), ϵ (such that), or $\therefore$ (therefore) in formal mathematical writing. It is often easier to write, and usually easier to read, if the English words are used instead of the sym- bols. For example, why make the reader interpret

   $$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = 0) \tag{3.1.5}$$

   When it is possible to write
   For each real number x, there exists a real number y such that $x + y = 0$, or, more succinctly (if appropriate),

   Every real number has an additive inverse.

Exercise for section 3.1

1. Prove each of the following statements:

   (a) For all integers a, b, and c with $a \neq 0$, if $a|b$ and $a|c$, then $a|(b - c)$.
   (b) For each $n \in \mathbb{Z}$, if n is an odd integer, then n^3 is an odd integer.
   (c) For each integer a, if 4 divides (a - 1), then 4 divides (a^2 - 1).
2. For each of the following, use a counterexample to prove the statement is false.

   (a) For each odd natural number n, if $n > 3$, then 3 divides (n^2 - 1).

(b) For each natural number n, $(3 \cdot 2^n + 2 \cdot 3^n + 1)$ is a prime number.
(c) For all real numbers x and y, $\sqrt{x^2 + y^2} > 2xy$.
(d) For each integer a, if 4 divides (a^2 - 1), then 4 divides (a - 1).

3. Determine if each of the following statements is true or false. If a statement is true, then write a formal proof of that statement, and if it is false, then provide a counterexample that shows it is false.

   (a) For all integers a, b, and c with $a \neq 0$, if $a|b$, then $a|(bc)$.
   (b) For all integers a and b with $a \neq 0$, if $6|(ab)$, then $6|a$ or $6|b$.
   (c) For all integers a, b and c with $a \neq 0$, if a divides (b - 1) and a divides (c -1), then a divides (bc - 1).
   (d) For each integer n, if 7 divides $(n^2 - 4)$, then 7 divides $(n - 2)$.
   (e) For every integer n, $4n^2 + 7n + 6$ is an odd integer.
   (f) For every odd integer n, $4n^2 + 7n + 6$ is an odd integer
   (g) For all integer a, b, and d with $d \neq 0$, if d divides both $a - b$ and $a + b$, then d divides a.
   (h) For all integer a, b, and c with $a \neq 0$, if $a|(bc)$, then $a|b$ or $a|c$.
4. (a) If x and y are integers and $xy = 1$, explain why $x = 1$ or $x = -1$.
   (b) Is the following proposition true or false?
   For all nonzero integers a and b, if $a|b$ and $b|a$, then $a = \pm b$.
5. Prove the following proposition:

   Let a be an integer. If there exists an integer n such that $a|(4n + 3)$ and $a|(2n + 1)$, then $a = 1$ or $a = -1$.

   Hint: Use the fact that the only divisors of 1 are 1 and -1.
6. Determine if each of the following statements is true or false. If a statement is true, then write a formal proof of that statement, and if it is false, then provide a counterexample that shows it is false. (a) For each integer a, if there exists an integer n such that a divides $(8n + 7)$ and a divides $(4n + 1)$, then a divides 5.
   (a) For each integer a, if there exists an integer n such that a divides $(9n + 5)$ and a divides $(6n + 1)$, then a divides 7.
   (c) For each integer n, if n is odd, then 8 divides $(n^4 + 4n^2 + 11)$.
   (d) For each integer n, if n is odd, then 8 divides $(n^4 + n^2 + 2n)$.
7. Let a be an integer and let $n \in \mathbb{N}$.

   (a) Prove that if $a \equiv 0$ (mod n), then $n|a$.
   (b) Prove that if $n|a$, then $a \equiv 0$ (mod n).
8. Let a and b be integers. Prove that if $a \equiv 2$ (mod 3) and $b \equiv 2$ (mod 3), then

   (a) $a + b \equiv 1$ (mod 3).
   (b) $a \cdot b \equiv 1$ (mod 3).
9. Let a and b be integers. Prove that if $a \equiv 7$ (mod 8) and $b \equiv 3$ (mod 8), then

   (a) $a + b \equiv 2$ (mod 8).
   (b) $a \cdot b \equiv 5$ (mod 8).
10. Determine if each of the following propositions is true or false. Justify each conclusion.

    (a) For all integers a and b, if $ab \equiv 0$ (mod 6), then $a \equiv 0$ (mod 6) or $b \equiv$ (mod 6).
    (b) For each integer a, if $a \equiv 2$ (mod 8), then $a^2 \equiv 4$ (mod 8).
    (c) For each integer a, if $a^2 \equiv 4$ (mod 8), then $a \equiv 2$ (mod 8).
11. Let n be a natural number. Prove each of the following:

    (a) For every integer a, $a \equiv a$ (mod n).
    This is called the **reflexive property** of congruence modulo n.
    (b) For every integer a and b, if $a \equiv b$ (mod n), then $b \equiv a$ (mod n).
    This is called the **symmetric property** of congruence modulo n.

(c) For every integer a, b and \9c\), if $a \equiv b$ (mod n) and $b \equiv c$ (mod n), then $a \equiv c$ (mod n).
This is called the **transitive property** of congruence modulo n.

12. Let n be a natural number and let a, b, c, and d be integers. Prove each of the following.

    (a) If $a \equiv b$ (mod n) and $c \equiv d$ (mod n), then $(a + c) \equiv (b + d)$ (mod n).
    (b) If $a \equiv b$ (mod n) and $c \equiv d$ (mod n), then $ac \equiv bd$ (mod n).

13. (a) Let a, b, and c be real numbers with $a \neq 0$. Explain how to use a part of the quadratic formula (called the discriminant) to determine if the quadratic equation $ax^2 + bx + c = 0$ has two real number solutions, one real number solution, or no real number solutions. (See Exercise (11) in Section 1.2 for a statement of the quadratic formula.)

    (b) Prove that if a, b, and c are real numbers for which $a > 0$ and $c < 0$, then one solution of the quadratic equation $ax^2 + bx + c = 0$ is a positive real number.

    (c) Prove that if a, b, and c are real numbers, if $a \neq 0$, $b > 0$ and $\dfrac{b}{2} < \sqrt{ac}$, then the quadratic equation $ax^2 + bx + c = 0$ has no real number solution.

14. Let h and k be real numbers and let r be a positive number. The equation for a circle whose center is at the point (h, k) and whose radius is r is

    $$(x - h)^2 + (y - k)^2 = r^2 \tag{3.1.6}$$

    .

    We also know that if a and b are real numbers, then

    - The point (a, b) is inside the circle if $(a - h)^2 + (b - k)^2 < r^2$.
    - The point (a, b) is on the circle if $(a - h)^2 + (b - k)^2 = r^2$.
    - The point (a, b) is outside the circle if $(a - h)^2 + (b - k)^2 > r^2$.

    Prove that all points on or inside the circle whose equation is $(x - 1)^2 + (y - 2)^2 = 4$ are inside the circle whose equation is $x^2 + y^2 = 26$.

15. Let r be a positive real number. The equation for a circle of radius r whose center is the origin is $x^2 + y^2 = r^2$.

    (a) Use implicit differentiation to determine $\dfrac{dy}{dx}$.
    (b) Let (a, b) be a point on the circle with $a \neq 0$ and $b \neq 0$. Determine the slope of the line tangent to the circle at the point (a, b).
    (c) Prove that the radius of the circle to the point (a, b) is perpendicular to the line tangent to the circle at the point (a, b).
    Hint: Two lines (neither of which is horizontal) are perpendicular if and only if the products of their slopes is equal to -1.

16. Determine if each of the following statements is true or false. Provide a counterexample for statements that are false and provide a complete proof for those that are true.

    (a) For all real numbers x and y, $\sqrt{xy} \le \dfrac{x + y}{2}$.
    (b) For all real numbers x and y, $xy \le (\dfrac{x + y}{2})^2$.
    (c) For all nonnegative real numbers x and y, $\sqrt{xy} \le \dfrac{x + y}{2}$.

17. Use one of the true in equalities in Exercise(16) to prove the following proposition.

    For each real number a, the value of x that gives the maximum value of $y = x(a - x)$ is $x = \dfrac{a}{2}$.

18. (a) State the Pythagorean Theorem for right triangles.
    The diagrams in Figure 3.1 will be used for the problems in this exercise.
    (b) In the diagram on the left, x is the length of a side of the equilateral triangle and h is the length of an altitude of the equilateral triangle. The labeling in the diagram shows the fact that the altitude intersects the base of the equilateral triangle at the midpoint of the base. Use the

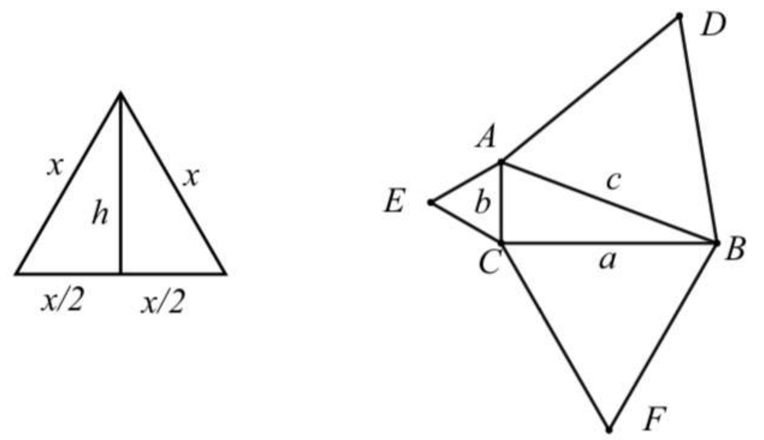


Figure 3.1: Diagrams for Exercise (18)

Pythagorean Theorem to prove that the area of this equilateral triangle is $\frac{\sqrt{3}}{4}x^2$.

(c) In the diagram on the right, $\triangle ABC$ is a right triangle. In addition, there has been an equilateral triangle constructed on each side of this right triangle. Prove that the area of the equilateral triangle on the hypotenuse is equal to the sum of the areas of the equilateral triangles constructed on the other two sides of the right triangle.

19. **Evaluation of proofs**

This type of exercise will appear frequently in the book. In each case, there is a proposed proof of a proposition. However, the proposition may be true or may be false.

- If a proposition is false, the proposed proof is, of course, incorrect. In this situation, you are to find the error in the proof and then provide a counterexample showing that the proposition is false.
- If a proposition is true, the proposed proof may still be incorrect. In this case, you are to determine why the proof is incorrect and then write a correct proof using the writing guidelines that have been presented in this book.
- If a proposition is true and the proof is correct, you are to decide if the proof is well written or not. If it is well written, then you simply must indicate that this is an excellent proof and needs no revision. On the other hand, if the proof is not well written, then you must then revise the proof so by writing it according to the guidelines presented in this text.

(a) **Proposition.** If m is an even integer, then $5m+4$ is an even integer.

Proof. We see that $5m+4=10n+4=2(5n+2)$. Therefore, $5m+4$ is an even integer.

(b) **Proposition.** For all real numbers x and y, if $x \neq y$, $x>0$, and $y>0$, then $\frac{x}{y}+\frac{y}{x}>2$.

Proof. Since x and y are positive real numbers, xy is positive and we can multiply both sides of the inequality by xy to obtain

$$\left(\frac{x}{y}+\frac{y}{x}\right)\cdot xy > 2\cdot xy \tag{3.1.7}$$

$$x^2+y^2>2xy \tag{3.1.8}$$

.

By combining all terms on the left side of the inequality, we see that $x^2-2xy+y^2>0$ and then by factoring the left side, we obtain $(x-y)^2>0$. Since $x \neq y$, $(x-y)\neq 0$ and so $(x-y)^2>0$. This proves that if $x\neq y$, $x>0$, and $y>0$, any $y>0$, then $\frac{x}{y}+\frac{y}{x}>2$.

(c) Proposition. For all integers a, b, and c, if $a|(bc)$, then $a|b$ or $a|c$.

Proof. We assume that a, b, and c are integers and that a divides bc. So, there exists an integer k such that $bc = ka$. We now factor k as $k = mn$, where m and n are integers. We then see that

$$bc = mna \tag{3.1.9}$$

.

This means that $b = ma$ or $c = na$ and hence, $a|b$ or $a|c$.

(d) Proposition. For all positive integers a, b, and c, $(a^b)^c = a^(b^c)$.
This proposition is false as is shown by the following counterexample: If we let $a = 2$, $b = 3$, and $c = 2$, then

$$(a^b)^c = a^{b^c} \tag{3.1.10}$$

$$(2^3)^2 = 2^{3^2} \tag{3.1.11}$$

$$8^2 = 2^9 \tag{3.1.12}$$

$$64 \neq 512 \tag{3.1.13}$$

Explorations and Activities

20. **Congruence Modulo 6**

    (a) Find several integers that are congruent to 5 modulo 6 and then square each of these integers.
    (b) For each integer m from Part (20a), determine an integer k so that $0 \le k < 6$ and $m^2 \equiv k$ (mod 6), then ...
    (c) Based on the work in Part (20b), complete the following conjecture:

    For each integer m, if $m \equiv 5$ (mod 6), then ...
    (d) Complete a know-show table for the conjecture in Part (20c) or write a proof of the conjecture.
21. **Pythagorean Triples**. Three natural numbers a, b, and c with $a < b < c$ are called a Pythagorean triple provided that $a^2 + b^2 = c^2$. See Exercise (13) on page 29 in Section 1.2. Three natural numbers are called **consecutive natural numbers** if they can be written in the form m, $m + 1$, and $m + 2$, where m is a natural number.

    (a) Determine all Pythagorean triples consisting of three consecutive natural numbers. (State a theorem and prove it.)
    (b) Determine all Pythagorean triples that can be written in the form m, $m + 7$, and $m + 8$, where m is a natural number. State a theorem and prove it.

Answer

Add texts here. Do not delete this text first.

This page titled 3.1: Direct Proofs is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

3.2: More Methods of Proof

? Preview Activity 1: Using the Contrapositive

The following statement was proven in Exercise (3c) on page 27 in Section 1.2.

If n is an odd integer, then n^2 is an odd integer.

Now consider the following proposition:

For each integer n, if n^2 is an odd integer, then n is an odd integer.

1. After examining several examples, decide whether you think this proposition is true or false.
2. Try completing the following know-show table for a direct proof of this proposition. The question is, “Can we perform algebraic manipulations to get from the ‘know’ portion of the table to the ‘show’ portion of the table?” Be careful with this! Remember that we are working with integers and we want to make sure that we can end up with an integer q as stated in Step $Q1$.

Step	Know	Reason
P	n^2 is an odd integer	Hypothesis
$P1$	$(\forall k \in \mathbb{Z})(n^2 = 2k + 1)$	Definition of "odd integer"
...	...	...
$Q1$	$(\forall q \in \mathbb{Z})(n = 2k + 1)$	
Q	n is an odd integer.	Definition of "odd integer"
Step	**Show**	**Reason**

Recall that the contrapositive of the conditional statement $P \rightarrow Q$ is the conditional statement $\urcorner Q \rightarrow \urcorner P$. We have seen in Section 2.2 that the contrapositive of a conditional statement is logically equivalent to the conditional statement. (It might be a good idea to review Preview Activity 3.2.2 from Section 2.2 on page 44.) Consider the following proposition once again:

For each integer n, if n^2 is an odd integer, then n is an odd integer.

3. Write the contrapositive of this conditional statement. Remember that “not odd” means “even.”
4. Complete a know-show table for the contrapositive statement from Part(3).
5. By completing the proof in Part (4), have you proven the given proposition? That is, have you proven that if n^2 is an odd integer, then n is an odd integer? Explain.

? Preview Activity 2: A Biconditional Statement

1. In Exercise (4a) from Section 2.2, we constructed a truth table to prove that the biconditional statement, $P \leftrightarrow Q$, is logically equivalent to $P \rightarrow Q) \wedge (Q \rightarrow P$. Complete this exercise if you have not already done so.
2. Suppose that we want to prove a biconditional statement of the form $P \leftrightarrow Q$. Explain a method for completing this proof based on the logical equivalency in part (1).
3. Let n be an integer. Assume that we have completed the proofs of the following two statements:
   - If n is an odd integer, then n2 is an odd integer.
   - If n2 is an odd integer, then n is an odd integer.

(See Exercise (3c) from Section 1.2 and Preview Activity 3.2.1.) Have we completed the proof of the following proposition?

For each integer n, n is an odd integer if and only if n^2 is an odd integer. Explain.

Review of Direct Proofs

In Sections 1.2 and 3.1, we studied direct proofs of mathematical statements. Most of the statements we prove in mathematics are conditional statements that can be written in the form $P \to Q$. A direct proof of a statement of the form $P \to Q$ is based on the definition that a conditional statement can only be false when the hypothesis, P, is true and the conclusion, Q, is false. Thus, if the conclusion is true whenever the hypothesis is true, then the conditional statement must be true. So, in a direct proof,

- We start by assuming that P is true.
- From this assumption, we logically deduce that Q is true.

We have used the so-called forward and backward method to discover how to logically deduce Q from the assumption that P is true.

Proof Using the Contrapositive

As we saw in Preview Activity $3.2.1$, it is sometimes difficult to construct a direct proof of a conditional statement. This is one reason we studied logical equivalencies in Section 2.2. Knowing that two expressions are logically equivalent tells us that if we prove one, then we have also proven the other. In fact, once we know the truth value of a statement, then we know the truth value of any other statement that is logically equivalent to it.

One of the most useful logical equivalencies in this regard is that a conditional statement $P \to Q$ is logically equivalent to its contrapositive, $\urcorner Q \to \urcorner P$. This means that if we prove the contrapositive of the conditional statement, then we have proven the conditional statement. The following are some important points to remember.

- A conditional statement is logically equivalent to its contrapositive.
- Use a direct proof to prove that $\urcorner Q \to \urcorner P$ is true.
- Caution: One difficulty with this type of proof is in the formation of correct negations. (We need to be very careful doing this.)
- We might consider using a proof by contrapositive when the statements P and Q are stated as negations.

Writing Guidelines

One of the basic rules of writing mathematical proofs is to keep the reader informed. So when we prove a result using the contrapositive, we indicate this within the first few lines of the proof. For example,

- We will prove this theorem by proving its contrapositive.
- We will prove the contrapositive of this statement.

In addition, make sure the reader knows the status of every assertion that you make. That is, make sure you state whether an assertion is an assumption of the theorem, a previously proven result, a well-known result, or something from the reader's mathematical background. Following is a completed proof of a statement from Preview Activity $3.2.1$.

Theorem 3.7

For each integer n, if n^2 is an even integer, then n is an even integer.

Proof

We will prove this result by proving the contrapositive of the statement, which is

For each integer n, if n is an odd integer, then n^2 is an odd integer.

However, in Theorem 1.8 on page 21, we have already proven that if x and y are odd integers, then $x \cdot y$ is an odd integer. So using $x = y = n$, we can conclude that if n is an odd integer, then $n \cdot n$, or n^2, is an odd integer. We have thus proved the contrapositive of the theorem, and consequently, we have proved that if n^2 is an even integer, then n is an even integer.

Using Other Logical Equivalencies

As was noted in Section 2.2, there are several different logical equivalencies. Fortunately, there are only a small number that we often use when trying to write proofs, and many of these are listed in Theorem 2.8 at the end of Section 2.2. We will illustrate the use of one of these logical equivalencies with the following proposition:

For all real numbers a and b, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.

First, notice that the hypothesis and the conclusion of the conditional statement are stated in the form of negations. This suggests that we consider the contrapositive. Care must be taken when we negate the hypothesis since it is a conjunction. We use one of De Morgan's Laws as follows:

$$\urcorner(a \neq 0 \wedge b \neq 0) \equiv (a=0) \vee (b=0). \tag{3.2.1}$$

? Progress Check 3.8 (Using Another Logical Equivalency)

1. In English, write the contrapositive of, "For all real numbers a and b, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$."

   The contrapositive is a conditional statement in the form $X \rightarrow (Y \vee Z$. The difficulty is that there is not much we can do with the hypothesis $ab=0$ since we know nothing else about the real numbers a and b. However, if we knew that a was not equal to zero, then we could multiply both sides of the equation $ab=0$ by $\frac{1}{a}$. This suggests that we consider using the following logical equivalency based on a result in Theorem 2.8 on page 48:

   $$X \rightarrow (Y \vee Z) \equiv (X \wedge \urcorner Y) \rightarrow Z. \tag{3.2.2}$$

2. In English, use this logical equivalency, to write a statement that is logically equivalent to the contrapositive from Part (1).

   The logical equivalency in Part (2) makes sense because if we are trying to prove $Y \vee Z$, we only need to prove that at least one of Y or Z is true. So the idea is to prove that if Y is false, then Z must be true.

3. Use the ideas presented in the progress check to complete the proof of the following proposition.

Proposition 3.9.

For all real numbers a and b, if $a \neq$ and $b \neq 0$, then $ab \neq 0$.

Proof

We will prove the contrapositive of this proposition, which is

For all real numbers a and b, if $ab=0$, then $a=0$ or $b=0$.

This contrapositive, however, is logically equivalent to the following:

For all real numbers a and b, if $ab=0$ and $a \neq 0$, then $b=0$.

To prove this, we let a and b be real numbers and assume that $ab=0$ and$a \neq 0$. We can then multiply both sides of the equation $ab=0$ by $\frac{1}{a}$. This gives

Now complete the proof.

...

Therefore, $b=0$. This completes the proof of a statement that is logically equivalent to the contrapositive, and hence, we have proven the proposition.

Answer

Add texts here. Do not delete this text first.

Proofs of Biconditional Statements

In Preview Activity $3.2.2$, we used the following logical equivalency:

$$(P \leftrightarrow Q) \equiv (P \rightarrow Q) \wedge (Q \rightarrow P). \tag{3.2.3}$$

This logical equivalency suggests one method for proving a biconditional statement written in the form "P if and only if Q." This method is to construct separate proofs of the two conditional statements $P \rightarrow Q$ and $Q \rightarrow P$. For example, since we have now proven each of the following:

- For each integer n, if n is an even integer, then n^2 is an even integer. (Exercise (3c) on page 27 in Section 1.2)

- For each integer n, if n^2 is an even integer, then n is an even integer. (Theorem 3.7)

We can state the following theorem.

Theorem 3.10.

For each integer n, n is an even integer if and only if n^2 is an even integer.

Writing Guidelines

When proving a biconditional statement using the logical equivalency $(P \leftrightarrow Q) \equiv (P \to Q) \wedge (Q \to P)$, we actually need to prove two conditional statements. The proof of each conditional statement can be considered as one of two parts of the proof of the biconditional statement. Make sure that the start and end of each of these parts is indicated clearly. This is illustrated in the proof of the following proposition.

Proposition 3.11

Let $x \in \mathbb{R}$. The real number x equals 2 if and only if $x^3 - 2x^2 + x = 2$.

Proof

We will prove this biconditional statement by proving the following two conditional statements:

- For each real number x, if x equals 2, then $x^3 - 2x^2 + x = 2$.
- For each real number x, if $x^3 - 2x^2 + x = 2$, then x equals 2.

For the first part, we assume $x = 2$ and prove that $x^3 - 2x^2 + x = 2$. We can do this by substituting $x = 2$ into the expression $x^3 - 2x^2 + x$. This gives

$$x^3 - 2x^2 + x = 2^3 - 2(2^2) + 2 = 8 - 8 + 2 = 2 \tag{3.2.4}$$

This completes the first part of the proof.

For the second part, we assume that $x^3 - 2x^2 + x = 2$ and from this assumption, we will prove that $x = 2$. We will do this by solving this equation for x. To do so, we first rewrite the equation $x^3 - 2x^2 + x = 2$ by subtracting 2 from both sides:

$$x^3 - 2x^2 + x - 2 = 0$$

We can now factor the left side of this equation by factoring an x from the first two terms and then factoring $(x - 2)$ from the resulting two terms. This is shown below.

$$x^3 - 2x^2 + x - 2 = 0$$

$$x^2(x - 2) + x - 2 = 0$$

$$(x - 2)(x^2 + 1) = 0$$

Now, in the real numbers, if a product of two factors is equal to zero, then one of the factors must be zero. So this last equation implies that

$$x - 2 = 0 \text{ or } x^2 + 1 = 0$$

The equation $x^2 + 1 = 0$ has not real numbers solution. So since x is a real number, the only possibility is that $x - 2 = 0$. From this we can conclude that x must be equal to 2.

Since we have now proven both conditional statements, we have proven that $x = 2$ if and only if $x^3 - 2x^2 + x = 2$

Constructive Proofs

We all know how to solve an equation such as $3x + 8 = 23$, where x is a real number. To do so, we first add -8 to both sides of the equation and then divide both sides of the resulting equation by 3. Doing so, we obtain the following result:

If x is a real number and $3x + 8 = 23$, then $x = 5$.

Notice that the process of solving the equation actually does not prove that $x = 5$ is a solution of the equation $3x + 8 = 23$. This process really shows that if there is a solution, then that solution must be $x = 5$. To show that this is a solution, we use the process of substituting 5 for x in the left side of the equation as follows: If $x = 5$,then

$$3x + 8 = 3(5) + 8 = 15 + 8 = 23$$

This proves that $x = 5$ is a solution of the equation $3x + 8 = 23$. Hence, we have proven that $x = 5$ is the only real number solution of $3x + 8 = 23$.

We can use this same process to show that any linear equation has a real number solution. An equation of the form

$$ax + b = c \tag{3.2.5}$$

,

where a, b, and c are real numbers with $a \neq 0$, is called a **linear equation in one variable.**

Proposition 3.12

If a, b, and c are real numbers with $a \neq 0$, then the linear equation $ax + b = c$ has exactly one real number solution, which is $x = \dfrac{c-b}{a}$.

Proof

Assume that a, b, and c are real numbers with $a \neq 0$. We can solve the linear equation $ax + b = c$ by adding $-b$ to both sides of the equation and then dividing both sides of the resulting equation by a (since $a \neq 0$, to obtain

$$x = \frac{c-b}{a}.$$

This shows that if there is a solution, then it must be $x = \dfrac{c-b}{a}$. We also see that if $x = \dfrac{c-b}{a}$, then,

$$ax + b = a(\frac{c-b}{a}) + b = (c-b) + b = c$$

Therefore, the linear equation $ax + b = c$ has exactly one real number solution and the solution is $x = \dfrac{c-b}{a}$.

The proof given for Proposition 3.12 is called a **constructive proof**. This is a technique that is often used to prove a so-called **existence theorem.** The objective of an existence theorem is to prove that a certain mathematical object exists. That is, the goal is usually to prove a statement of the form

There exists an x such that $P(x)$.

For a constructive proof of such a proposition, we actually name, describe, or explain how to construct some object in the universe that makes $P(x)$ true. This is what we did in Proposition 3.12 since in the proof, we actually proved that $\dfrac{c-b}{a}$ is a solution of the equation $ax + b = c$. In fact, we proved that this is the only solution of this equation.

Nonconstructive Proofs

Another type of proof that is often used to prove an existence theorem is the so- called **nonconstructive proof**. For this type of proof, we make an argument that an object in the universal set that makes $P(x)$ true must exist but we never construct or name the object that makes $P(x)$ true. The advantage of a constructive proof over a nonconstructive proof is that the constructive proof will yield a procedure or algorithm for obtaining the desired object.

The proof of the **Intermediate Value Theorem** from calculus is an example of a nonconstructive proof. The Intermediate Value Theorem can be stated as follows:

> If f is a continuous function on the closed interval $[a, b]$ and if q is any real number strictly between $f(a)$ and $f(b)$, then there exists a number c in the interval (a, b) such that $f(c) = q$.

The Intermediate Value Theorem can be used to prove that a solution to some equations must exist. This is shown in the next example.

Example 3.13 (Using the Intermediate Value Theorem)

Let x represent a real number. We will use the Intermediate Value Theorem to prove that the equation $x^3 - x + 1 = 0$ has a real number solution.

To investigate solutions of thee quation $x^3 - x + 1 = 0$, we will use the function

$$f(x) = x^3 - x + 1 = 0$$

Notice that $f(-2)$ = -5 and that $f(0)$ > 1. Since $f(-2)$ < 0 and $f(0$ > 0, the Intermediate Value Theorem tells us that there is a real number c between -2 and 0 such that $f(c) = 0$. This means that there exists a real number c between -2 and 0 such that

$$c^3 - c + 1 = 0,$$

and hence c is a real number solution of the equation $x^3 - x + 1 = 0$. This proves that the equation $x^3 - x + 1 = 0$ has at least one real number solution.

Notice that this proof does not tell us how to find the exact value of c. It does, however, suggest a method for approximating the value of c. This can be done by finding smaller and smaller intervals [a, b] such that $f(a)$ and $f(b)$ have opposite signs.

page128image3580513632 page128image3580513904

1. Let n be an integer. Prove each of the following:

   (a) If n is even, then n^3 is even.
   (b) If n^3 is even, then n is even.
   (c) The integer n is even if and only if n^3 is an even integer.
   (d) The integer n is odd if and only if n^3 is an odd integer.
2. In Section 3.1, we defined congruence modulo n where n is a natural number. If a and b are integers, we will use the notation $a \not\equiv b$ (mod n) to mean that a is not congruent to b modulo n.

   (a) Write the contrapositive of the following conditional statement:
   For all integers a and b, if $a \not\equiv 0$ (mod 6) and $b \not\equiv 0$ (mod 6), then $ab \not\equiv 0$ (mod 6).

   (b) Is this statement true or false? Explain.
3. (a) Write the contrapositive of the following statement:

   For all positive real numbers a and b, if $\sqrt{ab} \neq \dfrac{a+b}{2}$, then $a \neq b$.
   (b) Is this statement true or false? Prove the statement if it is true or provide a counterexample if it is false.
4. Are the following statements true or false? Justify your conclusions.
   (a) For each $a \in \mathbb{Z}$, if $a \equiv 2$ (mod 5), then $a^2 \equiv 4$ (mod 5).
   (b) For each $a \in \mathbb{Z}$, if $a^2 \equiv 4$ (mod 5), then $a \equiv 2$ (mod 5).
   (c) For each $a \in \mathbb{Z}$, $a \equiv 2$ (mod 5) if and only if $a^2 \equiv 4$ (mod 5).
5. Is the following proposition true or false?

   For all integers a and b, if ab is even, then a is even or b is even.

   Justify your conclusion by writing a proof if the proposition is true or by providing a counterexample if it is false.
6. Consider the following proposition: For each integer a, $a \equiv 3$ (mod 7) if and only if $(a^2 + 5a)) \equiv 3$ (mod 7).

   (a) Write the proposition as the conjunction of two conditional statements.
   (b) Determine if the two conditional statements in Part(a) are true or false. If a conditional statement is true, write a proof, and if it is false, provide a counterexample.
   (c) Is the given proposition true or false? Explain.

7. Consider the following proposition: For each integer a, $a \equiv 2 \pmod 8$ if and only if $(a^2 + 4a) \equiv 4 \pmod 8$.

   (a) Write the proposition as the conjunction of two conditional statements.
   (b) Determine if the two conditional statements in Part(a) are true or false. If a conditional statement is true, write a proof, and if it is false, provide a counterexample.
   (c) Is the given proposition true or false? Explain.
8. For a right triangle, suppose that the hypotenuse has length c feet and the lengths of the sides are a feet and b feet.

   (a) What is a formula for the area of this right triangle? What is an isosceles triangle?
   (b) State the Pythagorean Theorem for right triangles.
   (c) Prove that the right triangle describe above is an isosceles triangle if and only if the area of the right triangle is $\dfrac{1}{4}c^2$.
9. A real number x is defined to be a **rational number** provided

   there exist integers m and n with $n \neq 0$ such that $x = \dfrac{m}{n}$.

   A real number that is not a rational number is called an **irrational number**.It is known that if x is a positive rational number, then there exist positive integers m and n with $n \neq 0$ such that $x = \dfrac{m}{n}$
   Is the following proposition true or false? Explain.
   For each positive real number x, if x is irrational, then $\sqrt{x}$ is irrational.
10. Is the following proposition true or false? Justify your conclusion.

    For each integer n, n is even if and only if 4 divides n^2.
11. Prove that for each integer a, if $a^2 - 1$ is even, then 4 divides $a^2 - 1$.
12. Prove that for all integers a and m, if a and m are the lengths of the sides of a right triangle and $m + 1$ is the length of the hypotenuse, then a is an odd integer.
13. Prove the following proposition:

    If $p, q \in \mathbb{Q}$ with $p < q$, then there exists an $x \in \mathbb{Q}$ with $p < x < q$.
14. Are the following propositions true or false? Justify your conclusion.

    (a) There exist integers x and y such that $4x + 6y = 2$.
    (b) There exist integers x and y such that $6x + 15y = 2$.
    (c) There exist integers x and y such that $6x + 15y = 9$.
15. Prove that there exists a real number x such that $x^3 - 4x^2 = 7$.
16. Let y_1, y_2, y_3, y_4 be real numbers. The **mean**, $\bar{y}$, of these four numbers is defined to be the sum of the four numbers divided by 4, That is,

    $$\bar{y} = \frac{y_1 + y_2 + y_3 + y_4}{4}. \tag{3.2.6}$$

    Prove that there exists a y_i with $1 \leq i \leq 4$ such that $y_i \geq \bar{y}$.
    Hint: One way is to let y_{max} be the largest of y_1, y_2, y_3, y_4.
17. Let a and b be natural numbers such that $a^2 = b^3$. Prove each of the propositions in Parts (6a) trough (6d). (The results of Exercise (1) and Theorem 3.10 may be helpful.)

    (a) If a is even, then 4 divides a.
    (b) If 4 divides a, then 4 divides b.
    (c) If 4 divides b, then 8 divides a.
    (d) If a is even, then 8 divides a.
    (e) Given an example of natural numbers a and b such that a is even and $a^2 = b^3$, but b is not divisible by 8.

18. Prove the following proposition:
Let a and b be integers with $a \neq 0$. If a does not divide b, then the equation $ax^3 + bx + (b + a) = 0$ does not have a solution that is a natural number.
Hint: It may be necessary to factor a sum of cubes. Recall that

$$u^3 + v^3 = (u + v)(u^2 - uv + v^2). \tag{3.2.7}$$

19. **Evaluation of Proofs**
See the instructions for Excercise (19) on page 100 from Section 3.1.
(a)

proposition

If m is an odd integer, then $(m + 6)$ is an odd integer.

Proof

For $m + 6$ to be an odd integer, there must exist an integer n such that

$$m + 6 = 2n + 1. \tag{3.2.8}$$

By subtracting 6 from both sides of this equation, we obtain

$$m = 2n - 6 + 1 = 2(n - 3) = 1. \tag{3.2.9}$$

By the closure properties of the integers, $(n - 3)$ is an integer, and hence, the last equation implies that m is an odd integer. This proves that if m is an odd integer, then $m + 6$ is an odd integer.

(b)

proposition

For all integers m and n, if mn is an even integer, then m is even or n is even.

Proof

For either m or n to be even, there exists an integer k such that $m = 2k$ or $n = 2k$. So if we multiply m and n, the product will contain a factor of 2 and, hence, mn will be even.

Explorations and Activities

20. Using a Logical Equivalency. Consider the following proposition:
Proposition. For all integers a and b, if 3 does not divide a and 3 does not divide b, then 3 does not divide the product $a \cdot b$.

(a) Notice that the hypothesis of the proposition is stated as a conjunction of two negations ("3 does not divide a and 3 does not divide b"). Also, the conclusion is stated as the negation of a sentence ("3 does not divide the product $a \cdot b$."). This often indicates that we should consider using a proof of the contrapositive. If we use the symbolic form $(\urcorner Q \wedge \urcorner R) \to \urcorner P$ as a model for this proposition, what is P, what is Q, and what is R?
(b) Write a symbolic form for the contrapositive of $(\urcorner Q \wedge \urcorner R) \to \urcorner P$.
(c) Write the contrapositive of the proposition as a conditional statement in English.
We do not yet have all the tools needed to prove the proposition or its contrapositive. However, later in the text, we will learn that the following proposition is true.

Proposition X. Let a be an integer. If 3 does not divide a, then there exist integers x and y such that $3x + ay = 1$.

(d) i. Find integers x and y guaranteed by Proposition X when $a = 5$.
ii. Find integers x and y guaranteed by Proposition X when $a = 2$.

iii. Find integers x and y guaranteed by Proposition X when $a = -2$.

(e) Assume that Proposition X is true and use it to help construct a proof of the contrapositive of the given proposition. In doing so, you will most likely have to use the logical equivalency $P \to (Q \vee R) \equiv (P \wedge \urcorner Q) \to R$.

Answer

Add texts here. Do not delete this text first.

This page titled 3.2: More Methods of Proof is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

3.3: Proof by Contradiction

Preview Activity 1 (Proof by Contradiction)

In Section 2.1, we defined a **tautology** to be a compound statement S that is true for all possible combinations of truth values of the component statements that are part of S. We also defined **contradiction** to be a compound statement that is false for all possible combinations of truth values of the component statements that are part of S.

That is, a tautology is necessarily true in all circumstances, and a contradiction is necessarily false in all circumstances.

1. Use truth tables to explain why $P \vee \urcorner P$ is a tautology and $P \wedge \urcorner P$ is a contradiction.

   Another method of proof that is frequently used in mathematics is a **proof by contradiction**. This method is based on the fact that a statement X can only be true or false (and not both). The idea is to prove that the statement X is true by showing that it cannot be false. This is done by assuming that X is false and proving that this leads to a contradiction. (The contradiction often has the form $R \wedge \urcorner R$, where R is some statement.) When this happens, we can conclude that the assumption that the statement X is false is incorrect and hence X cannot be false. Since it cannot be false, then X must be true.
   A logical basis for the contradiction method of proof is the tautology

   $$[\urcorner X \rightarrow C] \rightarrow X, \tag{3.3.1}$$

   where X is a statement and C is a contradiction. The following truth table establishes this tautology.

X	C	$\urcorner X$	$\urcorner X \rightarrow C$	$(\urcorner X \rightarrow C) \rightarrow X$
T	F	F	T	T
F	F	T	F	T

   This tautology shows that if $\urcorner X$ leads to a contradiction, then X must be true. The previous truth table also shows that the statement $\urcorner X \rightarrow C$ is logically equivalent to X. This means that if we have proved that $\urcorner X$ leads to a contradiction, then we have proved statement X. So if we want to prove a statement X using a proof by contradiction, we assume that $\urcorner X$ is true and show that this leads to a contradiction.

   When we try to prove the conditional statement, “If P then Q” using a proof by contradiction, we must assume that $P \rightarrow Q$ is false and show that this leads to a contradiction.

2. Use a truth table to show that $\urcorner(P \rightarrow Q)$ is logical equivalent to $P \wedge \urcorner Q$.

   The preceding logical equivalency shows that when we assume that $P \rightarrow Q$ is false, we are assuming that P is true and Q is false. If we can prove that this leads to a contradiction, then we have shown that $\urcorner(P \rightarrow Q)$ is false and hence that $P \rightarrow Q$ is true.
3. Given a counterexample to show that the following statement is false.

   For each real number x, $\dfrac{1}{x(1-x)} \geq 4$.
4. When a statement is false, it is sometimes possible to add an assumption that will yield a true statement. This is usually done by using a conditional statement. So instead of working with the statement in (3), we will work with a related statement that is obtained by adding an assumption (or assumptions) to the hypothesis.

   For each real number x, if $0 < x < 1$, then $\dfrac{1}{x(1-x)} \geq 4$.
   To begin a proof by contradiction for this statement, we need to assume the negation of the statement. To do this, we need to negate the entire statement, including the quantifier. Recall that the negation of a statement with a universal quantifier is a statement that contains an existential quantifier. (See Theorem 2.16 on page 67). With this in mind, carefully write down all assumptions made at the beginning of a proof by contradiction for this statement.

Preview Activity 2 (Constructing a Proof by Contradiction)

Consider the following proposition:

Proposition. For all real numbers x and y, if $x \neq y$, $x > 0$, and $y > 0$, then $\frac{x}{y} + \frac{y}{x} > 2$.

To start a proof by contradiction, we assume that this statement is false; that is, we assume the negation is true. Because this is a statement with a universal quantifier, we assume that there exist real numbers x and y such that $x \neq y$, $x > 0$, $y > 0$ and that $\frac{x}{y} + \frac{y}{x} \le 2$. (Notice that the negation of the conditional sentence is a conjunction.)

For this proof by contradiction, we will only work with the know column of a know-show table. This is because we do not have a specific goal. The goal is to obtain some contradiction, but we do not know ahead of time what that contradiction will be. Using our assumptions, we can perform algebraic operations on the inequality

$$\frac{x}{y} + \frac{y}{x} \le 2 \tag{3.3.2}$$

until we obtain a contradiction.

1. Try the following algebraic operations on the inequality in (2). First, multiply both sides of the inequality by xy, which is a positive real number since $x > 0$ and $y > 0$. Then, subtract $2xy$ from both sides of this inequality and finally, factor the left side of the resulting inequality.
2. Explain why the last inequality you obtained leads to a contradiction.

By obtaining a contradiction, we have proved that the proposition cannot be false, and hence, must be true.

Writing Guidelines: Keep the Reader Informed

A very important piece of information about a proof is the method of proof to be used. So when we are going to prove a result using the contrapositive or a proof by contradiction, we indicate this at the start of the proof.

- We will prove this result by proving the contrapositive of the statement.
- We will prove this statement using a proof by contradiction.
- We will use a proof by contradiction.

We have discussed the logic behind a proof by contradiction in the preview activities for this section. The basic idea for a proof by contradiction of a proposition is to assume the proposition is false and show that this leads to a contradiction. We can then conclude that the proposition cannot be false, and hence, must be true. When we assume a proposition is false, we are, in effect, assuming that its negation is true. This is one reason why it is so important to be able to write negations of propositions quickly and correctly. We will illustrate the process with the proposition discussed in Preview Activity $3.3.1$.

Proposition 3.14

For each real number x, if $0 < x < 1$, then $\frac{1}{x(1-x)} \ge 4$

Proof

We will use a proof by contradiction. So we assume that the proposition is false, or that there exists a real number x such that $0 < x < 1$ and

$$\frac{1}{x(1-x)} < 4. \tag{3.3.3}$$

We note that since $0 < x < 1$, we can conclude that $x > 0$ and that $(1-x) > 0$. Hence, $x(1-x) > 0$ and if we multiply both sides of inequality (1) by $x(1-x)$, we obtain

$$1 < 4x(1-x).$$

We can now use algebra to rewrite the last inequality as follows:

$$1 < 4x - 4x^2$$

$$4x^2 - 4x + 1 < 0$$

$$(2x-1)^2 < 0$$

However, $(2x-1)$ is a real number and the last inequality says that a real number squared is less than zero. This is a contradiction since the square of any real number must be greater than or equal to zero. Hence, the proposition cannot be false, and we have proved that for each real number x, if $0 < x < 1$, then $\dfrac{1}{x(1-x)} \geq 4$.

? Progress Check 3.15: Starting a Proof by Contradiction

One of the most important parts of a proof by contradiction is the very first part, which is to state the assumptions that will be used in the proof by contradiction. This usually involves writing a clear negation of the proposition to be proven. Review De Morgan's Laws and the negation of a conditional statement in Section 2.2. (See Theorem 2.8 on page 48.) Also, review Theorem 2.16 (on page 67) and then write a negation of each of the following statements. (Remember that a real number is "not irrational" means that the real number is rational.)

1. For each real number x, if x is irrational, then $\sqrt[3]{x}$ is irrational.
2. For each real number x, $(x+\sqrt{2})$ is irrational or $(-x+\sqrt{2})$ is irrational.
3. For all integers a and b, if 5 divides ab, then 5 divides a or 5 divides b.
4. For all real numbers a and b, if $a > 0$ and $b > 0$, then $\dfrac{2}{a} + \dfrac{2}{b} \neq \dfrac{4}{a+b}$.

Answer

Add texts here. Do not delete this text first.

Important Note

A proof by contradiction is often used to prove a conditional statement $P \to Q$ when a direct proof has not been found and it is relatively easy to form the negation of the proposition. The advantage of a proof by contradiction is that we have an additional assumption with which to work (since we assume not only P but also $\urcorner Q$). The disadvantage is that there is no well-defined goal to work toward. The goal is simply to obtain some contradiction. There usually is no way of telling beforehand what that contradiction will be, so we have to stay alert for a possible absurdity. Thus, when we set up a know-show table for a proof by contradiction, we really only work with the know portion of the table.

? Progress Check 3.16: Exploration and a Proof by Contradiction

Consider the following proposition:

For each integer n, if $n \equiv 2 \pmod 4$, then $n \not\equiv 3 \pmod 6$.

1. Determine at least five different integers that are congruent to 2 modulo 4, and determine at least five different integers that are congruent to 3 modulo 6. Are there any integers that are in both of these lists?
2. For this proposition, why does it seem reasonable to try a proof by contradiction?
3. For this proposition, state clearly the assumptions that need to be made at the beginning of a proof by contradiction, and then use a proof by contradiction to prove this proposition.

Answer

Add texts here. Do not delete this text first.

Proving that Something Does Not Exist

In mathematics, we sometimes need to prove that something does not exist or that something is not possible. Instead of trying to construct a direct proof, it is sometimes easier to use a proof by contradiction so that we can assume that the something exists. For example, suppose we want to prove the following proposition:

Proposition 3.17.

For all integers x and y, if x and y are odd integers, then there does not exist an integer z such that $x^2 + y^2 = z^2$.

Notice that the conclusion involves trying to prove that an integer with a certain property does not exist. If we use a proof by contradiction, we can assume that such an integer z exists. This gives us more with which to work.

Progress Check 3.18

Complete the following proof of Proposition 3.17:

Proof. We will use a proof by contradiction. So we assume that there exist integers x and y such that x and y are odd and there exists an integer z such that $x^2+y^2=z^2$. Since x and y are odd, there exist integers m and n such that $x=2m+1$ and $y=2n+1$.

1. Use the assumptions that x and y are odd to prove that x^2+y^2 is even and hence, z^2 is even. (See Theorem 3.7 on page 105.)

   We can now conclude that z is even. (See Theorem 3.7 on page 105.) So there exists an integer k such that $z=2k$. If we substitute for x, y, and z in the equation $x^2+y^2=z^2$, we obtain

   $$(2m+1)^2+(2n+1)^2=(2k)^2. \tag{3.3.4}$$

2. Use the previous equation to obtain a contradiction. **Hint:** One way is to use algebra to obtain an equation where the left side is an odd integer and the right side is an even integer.

Answer

Add texts here. Do not delete this text first.

Rational and Irrational Numbers

One of the most important ways to classify real numbers is as a rational number or an irrational number. Following is the definition of rational (and irrational) numbers given in Exercise (9) from Section 3.2.

Definitions: Rational and Irrational Number

A real number x is defined to be a **rational number** provided that there exist integers m and n with $n \neq 0$ such that $x=\frac{m}{n}$. A real number that is not a rational number is called an **irrational number**.

This may seem like a strange distinction because most people are quite familiar with the rational numbers (fractions) but the irrational numbers seem a bit unusual. However, there are many irrational numbers such as $\sqrt{2}$, $\sqrt{3}$, $\sqrt[3]{2}$, π, and the number e. We are discussing these matters now because we will soon prove that $\sqrt{2}$ is irrational in Theorem 3.20.

We use the symbol $\mathbb{Q}$ to stand for the set of rational numbers. There is no standard symbol for the set of irrational numbers. Perhaps one reason for this is because of the closure properties of the rational numbers. We introduced closure properties in Section 1.1, and the rational numbers $\mathbb{Q}$ are closed under addition, subtraction, multiplication, and division by nonzero rational numbers. This means that if $x, y \in \mathbb{Q}$, then

- $x+y$, xy, and xy are in $\mathbb{Q}$; and
- If $y \neq 0$, then $\frac{x}{y}$ is in $\mathbb{Q}$.

The basic reasons for these facts are that if we add, subtract, multiply, or divide two fractions, the result is a fraction. One reason we do not have a symbol for the irrational numbers is that the irrational numbers are not closed under these operations. For example, we will prove that $\sqrt{2}$ is irrational in Theorem 3.20. We then see that

$$\sqrt{2}\sqrt{2}=2 \text{ and } \frac{\sqrt{2}}{\sqrt{2}}=1.$$

which shows that the product of irrational numbers can be rational and the quotient of irrational numbers can be rational.

It is also important to realize that every integer is a rational number since any integer can be written as a fraction. For example, we can write $3=\frac{3}{1}$. In general, if $n \in \mathbb{Z}$, then $n=\frac{n}{1}$, and hence, $n \in \mathbb{Q}$.

Because the rational numbers are closed under the standard operations and the definition of an irrational number simply says that the number is not rational, we often use a proof by contradiction to prove that a number is irrational. This is illustrated in the next proposition.

Proposition 3.19

For all real numbers x and y, if x is rational and $x \neq 0$ and y is irrational, then $x \cdot y$ is irrational.

Proof

We will use a proof by contradiction. So we assume that there exist real numbers x and y such that x is rational, y is irrational, and $x \cdot y$ is rational. Since $x \neq 0$, we can divide by x, and since the rational numbers are closed under division by nonzero rational numbers, we know that $\frac{1}{x} \in \mathbb{Q}$. We now know that $x \cdot y$ and $\frac{1}{x}$ are rational numbers and since the rational numbers are closed under multiplication, we conclude that

$$\frac{1}{x} \cdot (xy) \in \mathbb{Q} \tag{3.3.5}$$

However, $\frac{1}{x} \cdot (xy) = y$ and hence, y must be a rational number. Since a real number cannot be both rational and irrational, this is a contradiction to the assumption that y is irrational. We have therefore proved that for all real numbers x and y, if x is rational and $x \neq 0$ and y is irrational, then $x \cdot y$ is irrational.

The Square Root of 2 Is an Irrational Number

The proof that the square root of 2 is an irrational number is one of the classic proofs in mathematics, and every mathematics student should know this proof. This is why we will be doing some preliminary work with rational numbers and integers before completing the proof. The theorem we will be proving can be stated as follows:

Theorem 3.20

If r is a real number such that $r^2 = 2$, then r is an irrational number.

This is stated in the form of a conditional statement, but it basically means that $\sqrt{2}$ is irrational (and that $-\sqrt{2}$ is irrational). That is, $\sqrt{2}$ cannot be written as a quotient of integers with the denominator not equal to zero.

In order to complete this proof, we need to be able to work with some basic facts that follow about rational numbers and even integers.

1. Each integer m is a rational number since m can be written as $m = \frac{m}{1}$.
2. Notice that $\frac{2}{3} = \frac{4}{6}$, since

$$\frac{4}{6} = \frac{2 \cdot 2}{3 \cdot 2} = \frac{2}{2} \cdot \frac{2}{3} = \frac{2}{3} \tag{3.3.6}$$

   We can also show that $\frac{15}{12} = \frac{5}{4}$, $\frac{10}{-8} = \frac{-5}{4}$, and $\frac{-30}{-16} = \frac{15}{8}$
   Item (2) was included to illustrate the fact that a rational number can be written as a fraction in "lowest terms" with a positive denominator. This means that any rational number can be written as a quotient $\frac{m}{n}$, where m and n are integers, $n > 0$, and m and n have no common factor greater than 1.
3. If n is an integer and n^2 is even, what can be conclude about n. Refer to theorem 3.7 on page 105.

In a proof by contradiction of a conditional statement $P \to Q$, we assume the negation of this statement or $P \wedge \urcorner Q$. So in a proof by contradiction of Theorem 3.20, we will assume that r is a real number, $r^2 = 2$, and r is not irrational (that is, r is rational).

Theorem 3.20

If r is a real number such that $r^2 = 2$, then r is an irrational number.

Proof

We will use a proof by contradiction. So we assume that the statement of the theorem is false. That is, we assume that

r is a real number, $r^2 = 2$, and r is a rational number.

Since r is a rational number, there exist integers m and n with \(n > 0\0 such that

$$r = \frac{m}{n}$$

and m and n have no common factor greater than 1. We will obtain a contradiction by showing that m and n must both be even. Squaring both sides of the last equation and using the fact that $r^2 = 2$, we obtain

$$2 = \frac{m^2}{n^2}$$

$$m^2 = 2n^2 \tag{3.3.7}$$

Equation (1) implies that m^2 is even, and hence, by Theorem 3.7, m must be an even integer. This means that there exists an integer p such that $m = 2p$. We can now substitute this into equation (1), which gives

$$(2p)^2 = 2n^2$$

$$4p^2 = 2n^2. \tag{3.3.8}$$

We can divide both sides of equation (2) by 2 to obtain $n^2 = 2p^2$. Consequently, n^2 is even and we can once again use Theorem 3.7 to conclude that m is an even integer.

We have now established that both m and n are even. This means that 2 is a common factor of m and n, which contradicts the assumption that m and n have no common factor greater than 1. Consequently, the statement of the theorem cannot be false, and we have proved that if r is a real number such that $r^2 = 2$, then r is an irrational number.

Exercises for Section 3.3

1. This exercise is intended to provide another rationale as to why a proof by contradiction works.

   Suppose that we are trying to prove that a statement P is true. Instead of proving this statement, assume that we prove that the conditional statement “If $\urcorner P$, then C” is true, where C is some contradiction. Recall that a contradiction is a statement that is always false.

   (a) In symbols, write a statement that is a disjunction and that is logically equivalent to $\urcorner P \to C$.
   (b) Since we have proven that $\urcorner P \to C$ is true, then the disjunction in Exercise (1a) must also be true. Use this to explain why the statement P must be true.
   (c) Now explain why P must be true if we prove that the negation of P implies a contradiction.
2. Are the following statements true or false? Justify each conclusion.

   (a) For all integers a and b, if a is even and b is odd, then 4 does not divide $(a^2 + b^2)$.
   (b) For all integers a and b, if a is even and b is odd, then 6 does not divide $(a^2 + b^2)$.
   (c) For all integers a and b, if a is even and b is odd, then 4 does not divide $(a^2 + 2b^2)$.
   (d) For all integers a and b, if a is odd and b is odd, then 4 divides $(a^2 + 3b^2)$.
3. Consider the following statement:
   If r is a real number such that $r^2 = 18$, then r is irrational.

   (a) If you were setting up a proof by contradiction for this statement, what would you assume? Carefully write down all conditions that you would assume.
   (b) Complete a proof by contradiction for this statement.

4. Prove that the cube root of 2 is an irrational number. That is, prove that if r is a real number such that $r^3 = 2$, then r is an irrational number.
5. Prove the following propositions:

   (a) For all real numbers x and y, if x is rational and y is irrational, then $x + y$ is irrational.
   (b) For all nonzero real numbers x and y, if x is rational and y is irrational, then $\frac{x}{y}$ is irrational.
6. Are the following statements true or false? Justify each conclusion.

   (a) For each positive real number x, if x is irrational, then x^2 is irrational.
   (b) For each positive real number x, if x is irrational, then $\sqrt{x}$ is irrational.
   (c) For every pair of real numbers x and y, if $x + y$ is irrational, then x is irrational and y is irrational.
   (d) For every pair of real numbers x and y, if $x + y$ is irrational, then x is irrational or y is irrational.
7. (a) Give an example that shows that the sum of two irrational numbers can be a rational number.
   (b) Now explain why the following proof that $(\sqrt{2} + \sqrt{5})$ is an irrational number is not a valid proof: Since $\sqrt{2}$ and $\sqrt{5}$ are both irrational numbers, their sum is an irrational number. Therefore, $(\sqrt{2} + \sqrt{5})$ is an irrational number
   Note: You may even assume that we have proven that $\sqrt{5}$ is an irrational number. (We have not proven this.)
   (c) is the real number $\sqrt{2} + \sqrt{5}$ a rational number or an irrational number? Justify your conclusion.
8. (a) Prove that for each reach number x, $(x + \sqrt{2})$ is irrational or $(-x + \sqrt{2})$ is irrational.
   (b) Generalize the proposition in Part(a) for any irrational number (instead of just $\sqrt{2}$) and then prove the new proposition.
9. Is the following statement true or false?
   For all positive real number x and y, $\sqrt{x+y} \le \sqrt{x} + \sqrt{y}$.
10. Is the following proposition true or false? Justify your conclusion.
    For each real number x, $x(1-x) \le \frac{1}{4}$.
11. (a) Is the base 2 logarithm of 32, $log_2 32$, a rational number or an irrational number? Justify your conclusion.
    (b) Is the base 2 logarithm of 3, $log_2 3$, a rational number or an irrational number? Justify your conclusion.
12. In Exercise (15) in Section 3.2, we proved that there exists a real number solution to the equation $x^3 - 4x^2 = 7$. Prove that there is no integer x such that $x^3 - 4x^2 = 7$.
13. Prove each of the following propositions:

    (a) For each real number θ, if $0 < \theta < \frac{\pi}{2}$, then $(sin\theta + cos\theta) > 1$.
    (b) For all real numbers a and b, if $a \ne 0$ and $b \ne 0$, then $\sqrt{a^2 + b^2} \ne a + b$.
    (c) If n is an integer greater than 2, then for all integers m, n does not divide m or $n + m \ne nm$.
    (d) For all numbers a and b, if $a > 0$ and $b > 0$, then

$$\frac{2}{a} + \frac{2}{b} \ne \frac{4}{a+b}. \tag{3.3.9}$$

14. Prove that there do not exist three consecutive natural numbers such that the cube of the largest is equal to the sum of the cubes of the other two.
15. Three natural numbers a, b, and c with $a < b < c$ are called a **Pythagorean** triple provided that $a^2 + b^2 = c^2$. For example, the numbers 3, 4, and 5 form a Pythagorean triple, and the numbers 5, 12, and 13 form a Pythagorean triple.

    (a) Verify that if $a = 20$, $b = 21$, and $c = 29$, then $a^2 + b^2 = c^2$, and hence, 20, 21, and 29 form a Pythagorean triple.
    (b) Determine two other Pythagorean triples. That is, find integers a, b, and c such that $a^2 + b^2 = c^2$.
    (c) Is the following proposition true or false? Justify your conclusion.
    For all integers a, b, and c, if $a^2 + b^2 = c^2$, then a is even or b is even.
16. Consider the following proposition: There are no integers a and b such that $b^2 = 4a + 2$.

    (a) Rewrite this statement in an equivalent form using a universal quantifier by completing the following:
    For all integers a and b, ...
    (b) Prove the statement in Part (a).

17. Is the following statement true or false? Justify your conclusion.

    For each integer n that is greater than 1, if a is the smallest positive factor of n that is greater than 1, then a is prime.

    See Exercise (13) in Section 2.4 (page 78) for the definition of a prime number and the definition of a composite number.
18. A **magic square** is a square array of natural numbers whose rows, columns, and diagonals all sum to the same number. For example, the following is a 3 by 3 magic square since the sum of 3 numbers in each row is equal to 15, the sum of the 3 numbers in each column is equal to 15, and the sum of the 3 numbers in each diagonal is equal to 15.

8	3	4
1	5	9
6	7	2

Prove that the following 4 by 4 square cannot be completed to form a magic square.

	1		2
3	4	5	
6	7		8
9		10	

Hint: Assign each of the six blank cells in the square a name. One possibility is to use a, b, c, d, e, and f.

19. Using only the digits 1 through 9 one time each, is it possible to construct a 3 by 3 magic square with the digit 3 in the center square? That is, is it possible to construct a magic square of the form

a	b	c
d	3	e
f	g	h

where a, b, c, d, e, f, g, h are all distinct digits, none of which is equal to 3? Either construct such a magic square or prove that it is not possible.

20. **Evaluation of proofs**
    See the instructions for Exercise (19) on page 100 from Section 3.1

proposition

For each real number x, if x is irrational and m is an integer, then mx is irrational.

Proof

We assume that x is a real number and is irrational. This means that for all integers a and b with $b \neq 0$, $x \neq \frac{a}{b}$. Hence, we may conclude that $mx \neq \frac{ma}{b}$ and, therefore, mx is irrational.

proposition

For all real numbers x and y, if x is irrational and y is rational, then $x + y$ is irrational.

Proof

We will use a proof by contradiction. So we assume that the proposition is false, which means that there exist real numbers x and y where $x \notin \mathbb{Q}$, $y \in \mathbb{Q}$, and $x + y \in \mathbb{Q}$. Since the rational numbers are closed under subtraction and $x + y$ and y are rational, we see that

$$(x+y)-y\in\mathbb{Q} \tag{3.3.10}$$

.

However, $(x+y)-y=x$, and hence we can conclude that $x\in\mathbb{Q}$. This is a contradiction to the assumption that $x\notin\mathbb{Q}$. Therefore, the proposition is not false, and we have proven that for all real numbers x and y, if x is irrational and y is rational, then $x+y$ is irrational.

proposition

For each real number x, $x(1-x)\le\frac{1}{4}$.

Proof

A proof by contradiction will be used. So we assume the proposition is false. This means that there exists a real number x such that $x(1-x)>\frac{1}{4}$. If multiply both sides of this inequality by 4, we obtain $4x(1-x)>1$. However, if we let $x=3$, we then see that

$$\begin{gathered}4x(1-x)>1\\ 4\cdot 3(1-3)>1\\ -12>1\end{gathered}$$

The last inequality is clearly a contradiction and so we have proved the proposition.

Explorations and Activities

21. A Proof by Contradiction. Consider the following proposition:

Proposition. Let a, b, and c be integers. If 3 divides a, 3 divides b, and $c\equiv 1\pmod 3$, then the equation

$$ax+by=c$$

has not solution in which both x and y are integers.

Proof. A proof by contradiction will be used. So we assume that the statement is false. That is, we assume that there exist integers a, b, and c such that 3 divides both a and b, that $c\equiv 1\pmod 3$, and that the equation

$$ax+by=c$$

has a solution in which both x and y are integers. So there exist integers m and n such that

$$am+bn=c$$

Hint: Now use the facts that 3 divides a, 3 divides b, and $c\equiv 1\pmod 3$.

22. Exploring a Quadratic Equation. Consider the following proposition:

Proposition. For all integers m and n, if n is odd, then the equation

$$x^2+2mx+2n=0$$

has no integer solution for x.

(a) What are the solutions of the equation when $m=1$ and $n=1$? That is, what are the solutions of the equation $x^2+2x-2=0$?
(b) What are the solutions of the equation when $m=2$ and $n=3$? That is, what are the solutions of the equation $x^2+4x+2=0$?
(c) Solve the resulting quadratic equation for at least two more examples using values of m and n that satisfy the hypothesis of the proposition.
(d) For this proposition, why does it seem reasonable to try a proof by contradiction?
(e) For this proposition, state clearly the assumptions that need to be made at the beginning of a proof by contradiction.
(f) Use a proof by contradiction to prove this proposition.

Answer

Add texts here. Do not delete this text first.

This page titled 3.3: Proof by Contradiction is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

3.4: Using Cases in Proofs

PREVIEW ACTIVITY $3.4.1$: Using a Logical Equivalency

1. Complete a truth table to show that $(P \vee Q) \to R$ is logical equivalent to $(P \to R) \wedge (Q \to R)$.
2. Suppose that you are trying to prove a statement that is written in the form $(P \vee Q) \to R$. Explain why you can complete this proof by writing separate and independent proofs of $P \to R$ and $Q \to R$.
3. Now consider the following proposition:

   Proposition. For all integers x and y, if xy is odd, then x is odd and y is odd.
   Write the contrapositive of this proposition.
4. Now prove that if x is an even integer, then xy is an even integer. Also, prove that if y is an even integer, then xy is an even integer.
5. Use the results proved in part (4) and the explanation in part (2) to explain why we have proved the contrapositive of the proposition in part (3).

Preview Activity $3.4.1$: Using Cases in a Proof

The work in Preview Activity $3.4.1$ was meant to introduce the idea of using cases in a proof. The method of using cases is often used when the hypothesis of the proposition is a disjunction. This is justified by the logical equivalency

$$[(P \vee Q) \to R] \equiv [(P \to R) \wedge (Q \to R)] \tag{3.4.1}$$

See Theorem 2.8 on page 48 and Exercise (6) on page 50.

In some other situations when we are trying to prove a proposition or a theorem about an element x in some set U, we often run into the problem that there does not seem to be enough information about x to proceed. For example, consider the following proposition:

Proposition 1. If n is an integer, then $n^2 + n$ is an even integer.

If we were trying to write a direct proof of this proposition, the only thing we could assume is that n is an integer. This is not much help. In a situation such as this, we will sometimes use cases to provide additional assumptions for the forward process of the proof. Cases are usually based on some common properties that the element x may or may not possess. The cases must be chosen so that they exhaust all possibilities for the object x in the hypothesis of the original proposition. For Proposition 1, we know that an integer must be even or it must be odd. We can thus use the following two cases for the integer n:

- The integer n is an even integer;
- The integer n is an odd integer.

1. Complete the proof for the following proposition:

   Proposition 2: If n is an even integer, then $n^2 + n$ is an even integer.
   Proof. Let n be an even integer. Then there exists an integer m such that $n = 2m$. Substituting this into the expression $n^2 + n$ yields ...
2. Construct a proof for the following proposition:

   Proposition 3: If n is an odd integer, then $n^2 + n$ is an even integer.
3. Explain why the proofs of Proposition 2 and Proposition 3 can be used to construct a proof of Proposition 1.

Some Common Situations to Use Cases

When using cases in a proof, the main rule is that the cases must be chosen so that they exhaust all possibilities for an object x in the hypothesis of the original proposition. Following are some common uses of cases in proofs.

When the hypothesis is, "n is an integer."	Case 1: n is an even integer. Case 2: n is an odd integer.

When the hypothesis is, "m and n are integers."	Case 1: m and n are even. Case 2: m is even and n is odd. Case 3: m is odd and n is even. Case 4: m and n are both odd.
When the hypothesis is, "x is a real number."	Case 1: x is rational. Case 2: x is irrational.
When the hypothesis is, "x is a real number."	Case 1: $x = 0$ OR Case 1: $x > 0$ Case 2: $x \neq 0$ Case 2: $x = 0$ Case 3: $x < 0$
When the hypothesis is, "a and b are real numbers."	Case 1: $a = b$ OR Case 1: $a > b$ Case 2: $a \neq b$ Case 2: $a = b$ Case 3: $a < b$

Writing Guidelines for a Proof Using Cases

When writing a proof that uses cases, we use all the other writing guidelines. In addition, we make sure that it is clear where each case begins. This can be done by using a new paragraph with a label such as “Case 1,” or it can be done by starting a paragraph with a phrase such as, “In the case where . . . .”

? Progress Check 3.21: Using Cases: n Is Even or n Is Odd

Complete the proof of the following proposition:

Proposition. For each integer n, $n^2 - 5n + 7$ is an odd integer.

Proof. Let n be an integer. We will prove that $n^2 - 5n + 7$ is an odd integer by examining the case where n is even and the case where n is odd.

Case 1. The integer n is even. In this case, there exists an integer m such that $n = 2m$. Therefore, ...

Answer

Add texts here. Do not delete this text first.

As another example of using cases, consider a situation where we know that a and b are real numbers and $ab = 0$. If we want to make a conclusion about b, the temptation might be to divide both sides of the equation by a. However, we can only do this if $a \neq 0$. So, we consider two cases: one when $a = 0$ and the other when $a \neq 0$.

proposition 3.22

For all real numbers a and b, if $ab = 0$, then $a = 0$ or $b = 0$.

Proof

We let a and b be real numbers and assume that $ab = 0$. We will prove that $a = 0$ or $b = 0$ by considering two cases: (1) $a = 0$, and (2) $a \neq 0$.

In the case where $a = 0$, the conclusion of the proposition is true and so there is nothing to prove.

In the case where $a \neq 0$, we can multiply both sides of the equation $ab = 0$ by $dfrac1a$ and obtain

$$\frac{1}{a} \cdot ab = \frac{1}{a} \cdot 0$$

$$b = 0$$

So in both cases, $a = 0$ or $b = 0$, and this proves that for all real numbers a and b, if $ab = 0$, then $a = 0$ or $b = 0$.

Absolute Value

Most students by now have studied the concept of the absolute value of a real number. We use the notation $|x|$ to stand for the absolute value of the real number x. One way to think of the absolute value of x is as the "distance" between x and 0 on the number line. For example,

|-5| = 5 and |-7| = 7

Although this notion of absolute value is convenient for determining the absolute value of a specific number, if we want to prove properties about absolute value, we need a more careful and precise definition.

Definition: absolute value

For $x \in \mathbb{R}$, we define $|x|$, called the **absolute value of** x, by

$$|x| = \begin{cases} x & \text{if } x \geq 0; \\ -x & \text{if } x < 0. \end{cases}$$

Let's first see if this definition is consistent with our intuitive notion of absolute value by looking at two specific examples.

- Since 5 > 0, we see that |5| = 5, which should be no surprise.
- Since -7 < 0, we see that |-7| = -(-7) = 7.

Notice that the definition of the absolute value of x is given in two parts, one for when $x \geq 0$ and the other for when $x < 0$. This means that when attempting to prove something about absolute value, we often uses cases. This will be illustrated in Theorem 3.23.

Theorem 3.23

Let a be a positive real number. For each real number x,

1. $|x| = a$ if and only if $x = a$ or $x = -a$.
2. $|-x| = |x|$.

Proof

The proof of Part (2) is part of Exercise (10). We will prove Part (1).

We let a be a positive real number and let $x \in \mathbb{R}$. We will first prove that if $|x| = a$, then $x = a$ or $x = -a$. So we assume that $|x| = a$. In the case where $x \geq 0$, we see that $|x| = x$, and since $|x| = a$, we can conclude that $x = -a$.

In the case where $x < 0$, we see that $|x| = -x$. Since $|x| = a$, we can conclude that $-x = a$ and hence that $x = -a$. These two cases prove that if $|x| = a$, then $x = a$ or $x = -a$.

We will now prove that if $x = a$ or $x = -a$, then $|x| = a$. We start by assuming that $x = a$ or $x = -a$. Since the hypothesis of this conditional statement is a disjunction, we use two cases. When $x = a$, we see that

$$|x| = |a| = a \text{ since } a > 0.$$

When $x = -a$, we conclude that

$$|x| = |-a| = -(-a) \text{ since } -a < 0.$$

and hence, $|x| = a$. This proves that if $x = a$ or $x = -a$, then $|x| = a$. Because we have proven both conditional statements, we have proven that $|x| = a$ if and only if $x = a$ or $x = -a$.

Progress Check 3.24: Equations Involving Absolute Values

1. What is |4,3| and what is |-π|?
2. Use the properties of absolute value in Proposition 3.23 to help solve the following equations for t, where t is a real number.

   (a) $|t| = 12$.
   (b) $|t + 3| = 5$

(c) $|t-4| = \frac{1}{5}$.
(d) $|3t-4| = 8$.

Answer

Add texts here. Do not delete this text first.

Although solving equations involving absolute values may not seem to have anything to do with writing proofs, the point of Progress Check 3.24 is to emphasize the importance of using cases when dealing with absolute value. The following theorem provides some important properties of absolute value.

Theorem 3.25

Let a be a positive real number. For all real numbers x and y,

1. $|x| < a$ if and only if $-a < x < a$.
2. $|xy| = |x||y|$.
3. $|x+y| \leq |x| + |y|$. This is know as the ***Triangle Inequality.***

Proof

We will prove Part (1). The proof of Part (2) is included in Exercise (10), and the proof of Part (3) is Exercise (14). For Part (1), we will prove the biconditional proposition by proving the two associated conditional propositions.

So we let a be a positive real number and let $x \in \mathbb{R}$ and first assume that $|x| < a$. We will use two cases: either $x \geq 0$ or $x < 0$.

- In the case where $x \geq 0$, we know that $|x| = x$ and so the inequality $|x| < a$ implies that $x < a$. However, we also know that $-a < 0$ and that $x > 0$. Therefore, we conclude that $-a < x$ and, hence, $-a < x < a$.
- When $x < 0$, we see that $|x| = -x$. Therefore, the inequality $|x| < a$ implies that $-x < a$, which in turn implies that $-a < x$. In this case, we also know that $x < a$ since x is negative and a is positive. Hence, $-a < x < a$

So in both cases, we have proven that $-a < x < a$ and this proves that if $|x| < a$, then $-a < x < a$. We now assume that $-a < x < a$.

- If $x \geq 0$, then $|x| = x$ and hence, $|x| < a$.
- If $x < 0$, then $|x| = -x$ and so $|x| = -x$. Thus, $-a < -|x|$. By multiplying both sides of the last inequality by -1, we conclude that $|x| < a$.

These two cases prove that if $-a < x < a$, then $|x| < a$. Hence, we have proven that $|x| < a$ if and only if $-a < x < a$.

Exercises for section 3.4

1. In Preview Activity $3.4.2$, we proved that if n is an integer, then $n^2 + n$ is an even integer. We define two integers to be **consecutive integers** if one of the integers is one more than the other integer. This means that we can represent consecutive integers as m and $m+1$, where m is some integer.
   Explain why the result proven in Preview Activity $3.4.2$ can be used to prove that the product of any two consecutive integers is divisible by 2.
2. Prove that if u is an odd integer, then the equation $x^2 + x - u = 0$ has no solution that is an integer.
3. Prove that if n is an odd integer, then $n = 4k+1$ for some integer k or $n = 4k+3$ for some integer k.
4. Prove the following proposition:

   For each integer a, if $a^2 = a$, then $a = 0$ or $a = 1$.
5. (a) Prove the following proposition:
   For all integers a, b, and d with $d \neq 0$, if d divides a or d divides b, then d divides the product ab.
   Hint: Notice that the hypothesis is a disjunction. So use two cases.
   (b) Write the contrapositive of the proposition in Exercise(5a).
   (c) Write the converse of the proposition in Exercise (5a). Is the converse true or false? Justify your conclusion.

6. Are the following propositions true or false? Justify all your conclusions. If a biconditional statement is found to be false, you should clearly determine if one of the conditional statements within it is true. In that case, you should state an appropriate theorem for this conditional statement and prove it. (a) For all integers m and n, m and n are consecutive integers if and only if 4 divides $(m^2 + n^2 - 1$.
   (b) For all integers m and n, 4 divides $(m^2 - n^2)$ if and only if m and n are both even or m and n are both odd.
7. Is the following proposition true or false? Justify your conclusion with a counterexample or a proof.

   For each integer n, if n is odd, then $8|(n^2 - 1)$.
8. Prove that there are no natural numbers a and n with $n \geq 2$ and $a^2 + 1 = 2^n$.
9. Are the following propositions true or false? Justify each conclusions with a counterexample or a proof.

   (a) For all integers a and b with $a \neq 0$, the equation $ax + b = 0$ has a rational number solution.
   (b) For all integers a, b, and c, if a, b, and c are odd, then the equation $ax^2 + bx + c = 0$ has no solution that is a rational number.
   Hint: Do not use the quadratic formula. Use a proof by contradiction and recall that any rational number can be written in the form $\frac{p}{q}$, where p and q are integers, $q > 0$, and p and q have no common factor greater than 1.
   (c) For all integers a, b, c, and d, if a, b, c, and d are odd, then the equation $ax^3 + bx^2 + cx + d = 0$ has no solution that is a rational number.
10. (a) Prove Part (2) of Proposition 3.23.
    For each $x \in \mathbb{R}$, $|-x| = |x|$.
    (b) Prove Part (2) of Proposition 3.25.
    For all real numbers x and y, $|xy| = |x||y|$.
11. Let a be a positive real number. In Part (1) of Theorem 3.25, we proved that for each real number x, $|x| < a$ if and only if $-a < x < a$. It is important to realize that the sentence $-a < x < a$ is actually the conjunction of two inequalities. That is, $-a < x < a$ means that $-a < x$ and $x < a$.

    (a) Complete the following statement: For each real number x, $|x| \geq a$ if and only if ....
    (b) Prove that for each real number x, $|x| \leq a$ if and only if $-a \leq x \leq a$
    (c) Complete the following statement: For each real number x, $|x| > a$ if and only if ....
12. Prove each of the following:

    (a) For each nonzero real number x, $|x^{-1}| = \dfrac{1}{|x|}$.
    (b) For all real number x and y, $|x - y| \geq |x| - |y|$.
    Hint: An idea that is often used by mathematicians is to add 0 to an expression “intelligently”. In this case, we know that $(-y) + y = 0$. Start by adding this “version” of 0 inside the absolute value sign of $|x|$.
    (c) For all real number x and y, $||x| - |y|| \leq |x - y|$.
13. **Evaluation of proofs**
    See the instructions for Exercise (19) on page 100 from Section 3.1.

Theorem 3.4.1

The probabilities assigned to events by a distribution function on a sample space are given by.

Proof

Add proof here and it will automatically be hidden if you have a "AutoNum" template active on the page.

Theorem 3.4.1

The probabilities assigned to events by a distribution function on a sample space are given by.

Proof

Add proof here and it will automatically be hidden if you have a "AutoNum" template active on the page.

Explorations and Activities

14. **Proof of the Triangle Inequality.**

(a) Verify that the triangle inequality is true for several different real numbers x and y. Be sure to have some examples where the real numbers are negative.
(b) Explain why the following proposition is true: For each real number r, $-|r| \leq r \leq |r|$.
(c) Now let x and y be real numbers. Apply the result in Part (14b) to both x and y. Then add the corresponding parts of the two inequalities to obtain another inequality. Use this to prove that $|x+y| \leq |x|+|y|$.

Answer

Add texts here. Do not delete this text first.

This page titled 3.4: Using Cases in Proofs is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

3.5: The Division Algorithm and Congruence

? Preview Activity 1: Quotients and Remainders

1. Let $a = 27$ and $b = 4$. We will now determine several pairs of integers q and r so that $27 = 4q + r$. For example, if $q = 2$ and $r = 19$, we obtain $4 \cdot 2 + 19 = 27$. The following table is set up for various values of q. For each q, determine the value of r so that $4q + r = 27$.

q	1	2	3	4	5	6	7	8	9	10
r		19						-5		
$4q + r$	27	27	27	27	27	27	27	27	27	27

2. What is the smallest positive value for r that you obtained in your examples from Part (1)?

   Division is not considered an operation on the set of integers since the quotient of two integers need not be an integer. However, we have all divided one integer by another and obtained a quotient and a remainder. For example, if we divide 113 by 5, we obtain a quotient of 22 and a remainder of 3. We can write this as $\frac{113}{5} = 22 + \frac{3}{5}$. If we multiply both sides of this equation by 5 and then use the distributive property to "clear the parentheses," we obtain

$$5 \cdot \frac{113}{5} = 5(22 + \frac{3}{5})$$
$$113 = 5 \cdot 22 + 3$$

   This is the equation that we use when working in the integers since it involves only multiplication and addition of integers.

3. What are the quotient and the remainder when we divide 27 by 4? How is this related to your answer for Part (2)?
4. Repeat part (1) using $a = -17$ and $b = 5$. So the object is to find integers q and r so that $-17 = 5q + r$. Do this by completing the following table.

q	-7	-6	-5	-4	-3	-2	-1
r	18					-7	
$5q + r$	-17	-17	-17	-17	-17	-17	-17

5. The convention we will follow is that the remainder will be the smallest positive integer r for which $-17 = 5q + r$ and the quotient will be the corresponding value of q. Using this convention, what is the quotient and what is the remainder when -17 is divided by 5?

? Preview Activity 2: Some Work with Congruence Modulo n

1. Let n be a natural number and let a and b be integers.

   (a) Write the definition of "a is congruent to b modulo n," which is written $a \equiv b$ (mod n).

   (b) Use the definition of "divides" to complete the following:
   When we write $a \equiv b$ (mod n), we may conclude that there exists an integer k such that ....

   We will now explore what happens when we multiply several pairs of integers where the first one is congruent to 3 modulo 6 and the second is congruent to 5 modulo 6. We can use set builder notation and the roster method to specify the set A of all integers that are congruent to 2 modulo 6 as follows:

$$A = \{a \in \mathbb{Z} | a \equiv 3 \ (mod\ 6)\} = \{... - 15, -9, -3, 3, 9, 15, 21, ...\} \tag{3.5.1}$$

2. Use the roster method to specify the set B of all integers that are congruent to 5 modulo 6.

$$B = \{b \in \mathbb{Z} | b \equiv 5 \ (mod\ 6)\} = ... \tag{3.5.2}$$

Notice that $15 \in A$ and $11 \in B$ and that $15+11=26$. Also notice that $26 \equiv 2$ (mod 6) and that 2 is the smallest positive integer that is congruent to 26 (mod 6).

3. Now choose at least four other pairs of integers a and b where $a \in A$ and $b \in B$. For each pair, calculate $(a+b)$ and then determine the smallest positive integer r for which $(a+b) \equiv r$ (mod 6). **Note**: The integer r will satisfy the inequalities $0 \leq r$ < 6.
4. Prove that for all integers a and b, if $a \equiv 3$ (mod 6) and $b \equiv 5$ (mod 6), then $(a+b) \equiv 2$ (mod 6).

The Division Algorithm

Preview Activity 3.5.1 was an introduction to a mathematical result known as the Division Algorithm. One of the purposes of this preview activity was to illustrate that we have already worked with this result, perhaps without knowing its name. For example, when we divide 337 by 6, we often write

$$\frac{337}{6}=56+\frac{1}{6}.$$

When we multiply both sides of this equation by 6, we get

$$337=6 \cdot 56+1$$

When we are working within the system of integers, the second equation is preferred over the first since the second one uses only integers and the operations of addition and multiplication, and the integers are closed under addition and multiplication. Following is a complete statement of the Division Algorithm.

The Division Algorithm

For all integers a and b with $b>0$, there exist unique integers q and r such that

$$a=bq+r \text{ and } 0 \leq r<b$$

Some Comments about the Division Algorithm

1. The Division Algorithm can be proven, but we have not yet studied the methods that are usually used to do so. In this text, we will treat the Division Algorithm as an axiom of the integers. The work in Preview Activity 3.5.1 provides some rationale that this is a reasonable axiom.
2. The statement of the Division Algorithm contains the new phrase, “there exist unique integers q and r such that ....” This means that there is only one pair of integers q and r that satisfy both the conditions $a=bq+r$ and $0 \leq r<b$. As we saw in Preview Activity 3.5.1, there are several different ways to write the integer a in the form $a=bq+r$. However, there is only one way to do this and satisfy the additional condition that $0 \leq r<b$.
3. In light of the previous comment, when we speak of **the quotient** and **the remainder** when we “divide an integer a by the positive integer b,” we will always mean the quotient (q) and the remainder (r) guaranteed by the Division Algorithm. So the remainder r is the least nonnegative integer such that there exists an integer (quotient) q with $a=bq+r$.
4. If $a<0$, then we must be careful when writing the result of the Division Algorithm. For example, in parts (4) and (5) of Preview Activity 3.5.1, with $a=-17$ and $b=5$, we obtained $-17=5 \cdot(-4)+3$, and so the quotient is -4 and the remainder is 3. Notice that this is different than the result from a calculator, which would be $\frac{-17}{5}=-3.4$. But this means

   $$\frac{-17}{5}=-(3+\frac{4}{10})=-3-\frac{2}{5}. \tag{3.5.3}$$

   If we multiply both sides of this equation by 5, we obtain

   $$-17=5(-3)+(-2). \tag{3.5.4}$$

   This is not the result guaranteed by the Division Algorithm since the value of 2 does not satisfy the result of being greater than or equal to 0 and less than 5.
5. One way to look at the Division Algorithm is that the integer a is either going to be a multiple of b, or it will lie between two multiples of b. Suppose that a is not a multiple of b and that it lies between the multiples $b \cdot q$ and $b(q+1)$, where q is some integer. This is shown on the number line in Figure 3.2.

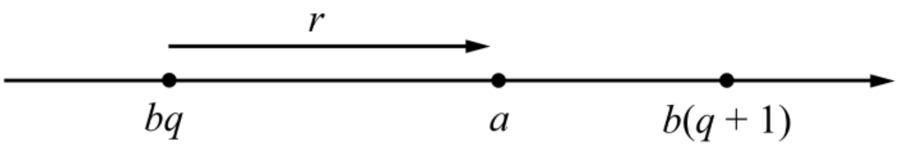


Figure 3.2: Remainder for the Division Algorithm

6. If r represents the distance from $b \cdot q$ to a, then

$$r = a - b \cdot q, or \tag{3.5.5}$$
$$a = b \cdot q + r. \tag{3.5.6}$$

   From the diagram, also notice that r is less than the distance between $b \cdot q$ and $b(q+1)$. Algebraically, this distance is

$$b(q+1) - b \cdot q = b \cdot q + b - b \cdot q \tag{3.5.7}$$
$$= b. \tag{3.5.8}$$

   Thus, in the case where a is not a multiple of b, we get $0 < r < b$.
7. We have been implicitly using the fact that an integer cannot be both even and odd. There are several ways to understand this fact, but one way is through the Division Algorithm. When we classify an integer as even or odd, we are doing so on the basis of the remainder (according to the Division Algorithm) when the integer is "divided" by 2. If $a \in \mathbb{Z}$, then by the Division Algorithm there exist unique integers q and r such that

   $a = 2q + r$ and $0 \le r < 2$.

   This means that the remainder, r, can only be zero or one (and not both). When $r = 0$, the integer is even, and when $r = 1$, the integer is odd.

? Progress Check 3.26: Using the Division Algorithm

1. What are the possible remainders (according to the Division Algorithm) when an integer is
   a. (a) Divided by 4?
   b. (b) Divided by 9?
2. For each of the following, find the quotient and remainder (guaranteed by the Division Algorithm) and then summarize the results by writing an equation of the form $a = bq + r$, where $0 \le r < b$.
   a. When 17 is divided by 3.
   b. When -17 is divided by 3.
   c. When 73 is divided by 7.
   d. When -73 is divided by 7.
   e. When 436 is divided by 27.
   f. When 539 is divided by 110.

Answer

Add texts here. Do not delete this text first.

Using Cases Determined by the Division Algorithm

The Division Algorithm can sometimes be used to construct cases that can be used to prove a statement that is true for all integers. We have done this when we divided the integers into the even integers and the odd integers since even integers have a remainder of 0 when divided by 2 and odd integers have a remainder o 1 when divided by 2.

Sometimes it is more useful to divide the integer a by an integer other than 2. For example, if a is divided by 3, there are three possible remainders: 0, 1, and 2. If a is divided by 4, there are four possible remainders: 0, 1, 2, and 3. The remainders form the basis for the cases.

If the hypothesis of a proposition is that "n is an integer," then we can use the Division Algorithm to claim that there are unique integers q and r such that

$$n = 3q + r \text{ and } 0 \leq r < 3$$

We can then divide the proof into the following three cases: (1) $r = 0$; (2) $r = 1$; and (3) $r = 2$. This is done in Proposition 3.27.

Proposition 3.27

If n is an integer, then 3 divides $n^3 - n$.

Proof

Let n be an integer. We will show that 3 divides $n^3 - n$ by examining the three cases for the remainder when n is divided by 3. By the Division Algorithm, there exist unique integers q and r such that

$$n = 3q + r, \text{ and } 0 \leq r < 3.$$

This means that we can consider the following three cases:(1) $r = 0$; (2) $r = 1$; and (3) $r = 2$.

In the case where $r = 0$, we have $n = 3q$. By substituting this into the expression $n^3 - n$, we get

$$\begin{aligned} n^3 - n &= (3q)^3 - (3q) \qquad (3.5.9) \\ &= 27q^3 - 3q \qquad (3.5.10) \\ &= 3(9q^3 - q). \qquad (3.5.11) \end{aligned}$$

Since $(9q^3 - q)$ is an integer, the last equation proves that $3|(n^3 - n)$.

In the second case, $r = 1$ and $n = 3q + 1$. When we substitute this into $(n^3 - n)$, we obtain

$$\begin{aligned} n^3 - n &= (3q + 1)^3 - (3q + 1) \qquad (3.5.12) \\ &= (27q^3 27q^2 + 27q + 1) - (3q + 1) \qquad (3.5.13) \\ &= 27q^3 + 27q^2 + 6q \qquad (3.5.14) \\ &= 3(9q^3 + 9q^2 + 2q). \qquad (3.5.15) \end{aligned}$$

Since $(9q^3 + 9q^2 + 2q)$ is an integer, the last equation proves that $3|(n^3 - n)$.

The last case is when $r = 2$. The details for this case are part of Exercise (1). Once this case is completed, we will have proved that 3 divides $n^3 - n$ in all three cases. Hence, we may conclude that if n is an integer, then 3 divides $n^3 - n$.

Properties of Congruence

Most of the work we have done so far has involved using definitions to help prove results. We will continue to prove some results but we will now prove some theorems about congruence (Theorem 3.28 and Theorem 3.30) that we will then use to help prove other results.

Let $n \in \mathbb{N}$. Recall that if a and b are integers, then we say that a is congruent to b modulo n provided that n divides $a - b$, and we write $a \equiv b \pmod{n}$. (See Section 3.1.) We are now going to prove some properties of congruence that are direct consequences of the definition. One of these properties was suggested by the work in Preview Activity $3.5.2$ and is Part (1) of the next theorem.

Theorem 3.28: Properties of Congruence Modulo n

Let n be a natural number and let a, b, c, and d be integers. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

1. $a + c) \equiv (b + d) \pmod{n}$.
2. $ac \equiv bd \pmod{n}$.
3. For each $m \in \mathbb{N}$, $a^m \equiv b^m \pmod{n}$.

Proof

We will prove Parts (2) and (3). The proof of Part (1) is Progress Check 3.29. Let n be a natural number and let a, b, c, and d be integers. Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. This means that n divides $a - b$ and that n divides $c - d$. Hence, there exist integers k and q such that $a-b=nk$ and $c-d=nq$. We can then write $a=b+nk$ and $c=d+nq$ and obtain

$$\begin{aligned} ac &= (b+nk)(d+nq) && (3.5.16)\\ &= bd+bnq+dnk+n^2kq && (3.5.17)\\ &= bd+n(bq+dk+nkq). && (3.5.18)\end{aligned}$$

by subtracting bd from both sides of the last equation, we see that

$$ac-bd=n(bq+dk+nkq). \tag{3.5.19}$$

Since $bq+dk+nkq$ is an integer, this proves that $n|(ac-bd)$, and hence we can conclude that $ac \equiv bd$ (mod n). This completes the proof of Part (2).

Part (2) basically means that if we have two congruences, we can multiply the corresponding sides of these congruences to obtain another congruence. We have assumed that $a \equiv$ ��b (mod n) and so we write this twice as follows:

$$\begin{aligned} a &\equiv b(mod\ n),\ \ and && (3.5.20)\\ a &\equiv b(mod\ n). && (3.5.21)\end{aligned}$$

If we now use the result in Part (2) and multiply the corresponding sides of these two congruences, we obtain $a^2 \equiv b^2$ (mod n). We can then use this congruence and the congruence $a \equiv b$ (mod n) and the result in Part (2) to conclude that

$$a^2 \cdot b \equiv b^2 \cdot b(mod\ n), \tag{3.5.22}$$

or that $a^3 \equiv b^3$ (mod n). We can say that we can continue with this process to prove Part (3), but this is not considered to be a formal proof of this result. To construct a formal proof for this, we could use a proof by mathematical induction. This will be studied in Chapter 4. See Exercise (13) in Section 4.1.

? Progress Check 3.29: Proving Part (1) of Theorem 3.28

Prove part (1) of Theorem 3.28.

Answer

Add texts here. Do not delete this text first.

Exercise (11) in Section 3.1 gave three important properties of congruence modulo n. Because of their importance, these properties are stated and proved in Theorem 3.30. Please remember that textbook proofs are usually written in final form of “reporting the news.” Before reading these proofs, it might be instructive to first try to construct a know-show table for each proof.

Theorem 3.30: Properties of Congruence Modulo n

Let $n \in \mathbb{N}$, and let a, b, and c be integers.

1. For every integer a, $a \equiv a$ (mod n).
   This is called the ***reflexive property*** of congruence modulo n.
2. If $a \equiv b$ (mod n), then $b \equiv a$ (mod n).
   This is called ***symmetric property*** of congruence modulo n.
3. If $a \equiv b$ (mod n) and $b \equiv c$ (mod n), then $a \equiv c$ (mod n).
   This is called ***transitive property*** of congruence modulo n.

Proof

We will prove the reflexive property and the transitive property. The proof of the symmetric property is Exercise (3).

Let $n \in \mathbb{N}$, and let $a \in \mathbb{Z}$. We will show that $a \equiv a$ (mod n). Notice that

$$a-a=0=n\cdot 0. \tag{3.5.23}$$

This proves that n divides $a-a$ and hence, by the definition of congruence modulo n, we have proven that $a \equiv a$ (mod n).

To prove the transitive property, we let $n \in \mathbb{N}$, and let a, b, and c be integers. We assume that $a \equiv b$ (mod n) and $b \equiv c$ (mod n). We will use the definition of congruence modulo n to prove that $a \equiv c$ (mod n). Since $a \equiv b$ (mod n) and $b \equiv c$ (mod n), we know that $n|(a-b)$ and $n|(b-c)$. Hence, there exist integers k and q such that

$$a - b = nk \tag{3.5.24}$$
$$b - c = nq. \tag{3.5.25}$$

by adding the corresponding sides of these two equations, we obtain

$$(a-b)+(b-c) = nk + nq. \tag{3.5.26}$$

If we simplify the left side of the last equation and factor the right side, we get

$$a - c = n(k+q). \tag{3.5.27}$$

By the closure property of the integers, $(k+q) \in \mathbb{Z}$, and so this equation proves that $n|(a-c)$ and hence that $a \equiv c$ (mod n). This completes the proof of the transitive property of congruence modulo n.

Using Cases Based on Congruence Modulo n

Notice that the set of all integers that are congruent to 2 modulo 7 is

$$\{n \in \mathbb{Z} | n \equiv 2 \ (mod\ 7)\} = \{\ldots, -19, -12, -5, 2, 9, 16, 23, \ldots\} \tag{3.5.28}$$

If we divide any integer in this set by 7 and write the result according to the Division Algorithm, we will get a remainder of 2. For example,

$$2 = 7 \cdot 0 + 2 \tag{3.5.29}$$
$$9 = 7 \cdot 1 + 2 \tag{3.5.30}$$
$$16 = 7 \cdot 2 + 2 \tag{3.5.31}$$
$$23 = 7 \cdot 3 + 2 \tag{3.5.32}$$
$$-5 = 7(-1) + 2 \tag{3.5.33}$$
$$-12 = 7(-2) + 2 \tag{3.5.34}$$
$$-19 = 7(-3) + 2 \tag{3.5.35}$$

Is this a coincidence or is this always true? Let's look at the general case. For this, let n be a natural number and let $a \in \mathbb{Z}$. By the Division Algorithm, there exist unique integers q and r such that

$$a = nq + r \text{ and } 0 \le r < n.$$

By subtracting r from both sides of the equation $a = nq + r$, we obtain

$$a - r = nq.$$

But this implies that $n|(a-r)$ and hence that $a \equiv r$ (mod n). We have proven the following result.

Theorem 3.31

Let $n \in \mathbb{N}$ and let $a \in mathbbZ$. If $a = nq + r$ and $0 \le r < n$ for some integers q and r, then $a \equiv r$ (mod n).

This theorem says that an integer is congruent (mod n) to its remainder when it is divided by n. Since this remainder is unique and since the only possible remainders for division by n are 0, 1, 2,..., n1, we can state the following result.

Corollary 3.32

If $n \in \mathbb{N}$, then each integer is congruent, modulo n, to precisely one of the integers 0, 1, 2, ..., $n-1$. That is, for each integer a, there exists a unique integer r such that

$$a \equiv r \text{ (mod } n\text{) and } 0 \le r < n.$$

Corollary 3.32 can be used to set up cases for an integer in a proof. If $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, then we can consider n cases for a. The integer a could be congruent to 0,1, 2, ..., or $n-1$ modulo n. For example, if we assume that 5 does not divide an integer a, then we know a is not congruent to 0 modulo 5, and hence, that a must be congruent to 1, 2, 3, or 4 modulo 5. We can use these as 4 cases within a proof. For example, suppose we wish to determine the values of a^2 modulo 5 for integers that are not congruent to 0 modulo 5. We begin by squaring some integers that are not congruent to 0 modulo 5. We see that

$$1^2 = 1 \quad \text{and} \quad 1 \equiv 1\ (mod\ 5). \tag{3.5.36}$$

$$3^2 = 9 \quad \text{and} \quad 9 \equiv 4\ (mod\ 5). \tag{3.5.37}$$

$$6^2 = 36 \quad \text{and} \quad 36 \equiv 1\ (mod\ 5). \tag{3.5.38}$$

$$8^2 = 64 \quad \text{and} \quad 64 \equiv 4\ (mod\ 5). \tag{3.5.39}$$

$$9^2 = 81 \quad \text{and} \quad 81 \equiv 1\ (mod\ 5). \tag{3.5.40}$$

These explorations indicate that the following proposition is true and we will now outline a method to prove it.

Proposition 3.33.

For each integer a, if $a \not\equiv 0$ (mod 5), then $a^2 \equiv 1$ (mod 5) or \(a^2 \equiv 4) (mod 5).

Proof

We will prove this proposition using cases for a based on congruence modulo 5. In doing so, we will use the results in Theorem 3.28 and Theorem 3.30. Because the hypothesis is $a \not\equiv 0$ (mod 5), we can use four cases, which are: (1)$a \equiv 1$ (mod 5), (2)$a \equiv 2$ (mod 5), (3)$a \equiv 3$ (mod 5), and (4)\(a \equiv 4) (mod 5). Following are proofs for the first and fourth cases.

Case 1. ($a \equiv 1$ (mod 5)). In this case, we use Theorem 3.28 to conclude that

$$a^2 \equiv 1^2 \text{ (mod 5) or } a^2 \equiv 1 \text{ (mod 5).}$$

This proves that if $a \equiv 1$ (mod 5), then $a^{\equiv}1$ (mod 5).

Case 4. ($a \equiv 4$ (mod 5)). In this case, we use Theorem 3.28 to conclude that

$$a^2 \equiv 4^2 \text{ (mod 5) or } a^2 \equiv 16 \text{ (mod 5).}$$

We also know that $16 \equiv 1$ (mod 5). So we have $a^2 \equiv 16$ (mod 5) and $16 \equiv 1$ (mod 5), and we can now use the transitive property of congruence (Theorem 3.30) to conclude that $a^2 \equiv 1$ (mod 5). This proves that if $a \equiv 4$ (mod 5), then $a^2 \equiv 1$ (mod 5).

Progress Check 3.34 (Using Properties of Congruence)

Complete a proof of Proposition 3.33 by completing proofs for the other two cases.

Note: It is possible to prove Proposition 3.33 using only the definition of congruence instead of using the properties that we have proved about congruence. However, such a proof would involve a good deal of algebra. One of the advantages of using the properties is that it avoids the use of complicated algebra in which it is easy to make mistakes.

Answer

Add texts here. Do not delete this text first.

In the proof of Proposition 3.33, we used four cases. Sometimes it may seem a bit overwhelming when confronted with a proof that requires several cases. For example, if we want to prove something about some integers modulo 6, we may have to use six cases. However, there are sometimes additional assumptions (or conclusions) that can help reduce the number of cases that must be considered. This will be illustrated in the next progress check.

Progress Check 3.35: Using Cases Modulo 6

Suppose we want to determine the possible values for a^2 modulo 6 for odd integers that are not multiples of 3. Before beginning to use congruence arithmetic (as in the proof of Proposition 3.33) in each of the possible six cases, we can show that some of the cases are not possible under these assumptions. (In some sense, we use a short proof by contradiction for these cases.) So assume that a is an odd integer. Then:

- If $a \equiv 0$ (mod 6), then there exists an integer k such that $a = 6k$. But then $a = 2(3k)$ and hence, a is even. Since we assumed that a is odd, this case is not possible.

- If $a \equiv 2 \pmod 6$, then there exists an integer k such that $a = 6k + 2$. But then $a = 2(3k + 1)$ and hence, a is even. Since we assumed that a is odd, this case is not possible.

1. Prove that if a is an odd integer, then a cannot be congruent to 4 modulo 6.
2. Prove that if a is an integer and 3 does not divide a, then a cannot be congruent to 3 modulo 6.
3. So if a is an odd integer that is not a multiple of 3, then a must be congruent to 1 or 5 modulo 6. Use these two cases to prove the following proposition:

Answer

Add texts here. Do not delete this text first.

Proposition 3.36.

For each integer a, if a is an odd integer that is not multiple of 3, then $a^2 \equiv 1 \pmod 6$.

Exercises for Section 3.5

1. Complete the details for the proof of Case 3 of Proposition 3.27.
2. Extending the idea in Exercise (1) of Section 3.4, we can represent three consecutive integers as m, $m+1$, and $m+2$, where m is an integer.

   (a) Explain why we can also represent three consecutive integers as $k-1$, k, and $k+1$, where k is an integer.
   (b) Explain why Proposition 3.27 proves that the product of any three consecutive integers is divisible by 3.
   (c) Prove that the product of three consecutive integers is divisible by 6.
3. Prove the symmetric property of congruence stated in Theorem 3.30.
4. (a) Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$. Explain why n divides a if and only if $a \equiv 0 \pmod n$.
   (b) Let $a \in \mathbb{Z}$. Explain why if $a \not\equiv 0 \pmod 3$, then $a \equiv 1 \pmod 3$ or $a \equiv 2 \pmod 3$.
   (c) Is the following proposition true or false? Justify your conclusion.
   For each $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod 3$ if and only if $a^2 \equiv 1 \pmod 3$.
5. (a) Use cases based on congruence modulo 3 and properties of congruence to prove that for each integer n, $n^3 \equiv n \pmod 3$.
   (b) Explain why the result in Part (a) proves that for each integer n, 3 divides $n^3 - n$. Compare this to the proof of the same result in Proposition 3.27.
6. Prove that for each natural number n, $\sqrt{3n+2}$ is not a natural number.
7. Prove the following proposition by proving its contrapositive. (**Hint**: Use case analysis. There are several cases.

   For all integers a and b, if $ab \equiv 0 \pmod 3$, then $a \equiv 0 \pmod 3$ or $b \equiv 0 \pmod 3$.
8. (a) Explain why the following proposition is equivalent to the proposition in Exercise (7).
   For all integers a and b, if $3|ab$, then $3|a$ or $3|b$.
   (b) Prove that for each integer a, if 3 divides a^2, then 3 divides a.
9. (a) Prove that the real number $\sqrt{3}$ is an irrational number. That is, prove that
   If r is a positive real number such that $r^2 = 3$, then r is irrational.
   (b) Prove that the real number $\sqrt{12}$ is an irrational number.
10. (a) Use the result in Proposition 3.33 to help prove that the integer m = 5, 344, 580, 232, 468, 953, 153 is not a perfect square. Recall that an integer n is a perfect square provided that there exists an integer k such that $n = k^2$. **Hint**: Use a proof by contradiction.
    (b) Is the integer n = 782, 456, 231, 189, 002, 288, 438 a perfect square? Justify your conclusion.
11. (a) Use the result in Proposition 3.33 to help prove that for each integer a, if 5 divides a^2, then 5 divides a.
    (b) Prove that the real number $\sqrt{5}$ is an irrational number.
12. (a) Prove that for each integer a, if $a \not\equiv 0 \pmod 7$, then $a^2 \not\equiv 0 \pmod 7$.
    (b) Prove that for each integer a, if 7 divides a^2, then 7 divides a.
    (c) Prove that the real number $\sqrt{7}$ is an irrational number.

13. (a) If an integer has a remainder of 6 when it is divided by 7, is it possible to determine the remainder of the square of that integer when it is divided by 7? If so, determine the remainder and prove that your answer is correct.
    (b) If an integer has a remainder of 11 when it is divided by 12, is it possible to determine the remainder of the square of that integer when it is divided by 12? If so, determine the remainder and prove that your answer is correct.
    (c) Let n be a natural number greater than 2. If an integer has a remainder of $n-1$ when it is divided by n, is it possible to determine the remainder of the square of that integer when it is divided by n? If so, determine the remainder and prove that your answer is correct.
14. Let n be a natural number greater than 4 and let a be an integer that has a remainder of $n-2$ when it is divided by n. Make whatever conclusions you can about the remainder of a^2 when it is divided by n. Justify all conclusions.
15. Is the following proposition true or false? Justify your conclusion with a proof or a counterexample.
    For each natural number n, if 3 does not divide (n^2+2), then n is not a prime number or $n=3$.
16. (a) Is the following proposition true or false? Justify your conclusion with a counterexample or a proof.
    For each integer n, if n is odd then $n^2 \equiv 1$ (mod 8).
    (b) Compare this proposition to the proposition in Exercise (7) from Section 3.4. Are these two propositions equivalent? Explain.
    (c) Is the following proposition true or false? Justify your conclusion with a counterexample or a proof.
    For each integer n, if n is odd and n is not a multiple of 3, then $n^2 \equiv 1$ (mod 24).
17. Prove the following proposition:
    For all integers a and b, if 3 divides (a^2+b^2), then 3 divides a and 3 divides b.
18. Is the following proposition true or false? Justify your conclusion with a counterexample or a proof.
    For each integer a, 3 divides a^3+23a.
19. Are the following statements true or false? Either prove the statement is true or provide a counterexample to show it is false.

    (a) For all integer a and b, if $a \cdot b \equiv 0$ (mod 6), then $a \equiv 0$ (mod 6) or $b \equiv 0$ (mod 6).
    (b) For all integer a and b, if $a \cdot b \equiv 0$ (mod 8), then $a \equiv 0$ (mod 8) or $b \equiv 0$ (mod 8).
    (c) For all integer a and b, if $a \cdot b \equiv 1$ (mod 6), then $a \equiv 1$ (mod 6) or $b \equiv 1$ (mod 6).
    (d) For all integer a and b, if $ab \equiv 7$ (mod 6), then either $a \equiv 1$ (mod 12) or $b \equiv 7$ (mod 12).
20. (a) Determine several pairs of integers a and b such that $a \equiv b$ (mod 5). For each such pair, calculate $4a+b$, $3a+2b$, and $7a+3b$. Are each of the resulting integers congruent to 0 modulo 5?
    (b) Prove or disprove the following proposition:
    Let m and n be integers such that $(m+n) \equiv 0$ (mod 5) and let $a, b \in \mathbb{Z}$. If $a \equiv b$ (mod 5), then $(ma+nb) \equiv 0$ (mod 5).
21. **Evaluation of proofs**
    See the instructions for Exercise (19) on page 100 from Section 3.1.
    (a)

Proposition

For all integers a and b, if $(a+2b) \equiv 0$ (mod 3), then $(2a+b) \equiv 0$ (mod 3).

Proof

We assume $a, b \in \mathbb{Z}$ and $(a+2b) \equiv 0$ (mod 3). This means that 3 divides $a+2b$ and, hence, there exists an integer m such that $a+2b=3m$. Hence, $a=3m-2b$. For $(2a+b) \equiv 0$ (mod 3), there exists an integer x such that $2a+b=3x$. Hence,

$$\begin{aligned} 2(3m-2b)+b &= 3x && (3.5.41)\\ 6m-3b &= 3x && (3.5.42)\\ 3(2m-b) &= 3x && (3.5.43)\\ 2m-b &= x && (3.5.44) \end{aligned}$$

Since $(2m-b)$ is an integer, this proves that 3 divides $(2a+b)$ and hence, $(2a+b) \equiv 0$ (mod 3)

(b)

Proposition.

For each integer m, 5 divides $(m^5 - m)$.

Proof

Let $m \in \mathbb{Z}$. We will prove that 5 divides $(m^5 - m)$ by proving that divides $(m^5 - m) \equiv 0$ (mod 5). We will use cases.

For the first case, if $m \equiv 0$ (mod 5), then $m^5 \equiv 0$ (mod 5) and, hence, ((m^5 - m) \equiv 0\) (mod 5).

For the second case, if $m \equiv 1$ (mod 5), then $m^5 \equiv 1$ (mod 5) and, hence, ((m^5 - m) \equiv (1 - 1)\) (mod 5), which means that ((m^5 - m) \equiv 0\) (mod 5).

For the third case, if $m \equiv 2$ (mod 5), then $m^5 \equiv 32$ (mod 5) and, hence, ((m^5 - m) \equiv (32 - 2)\) (mod 5), which means that ((m^5 - m) \equiv 0\) (mod 5).

Explorations and Activities

22. **Using a Contradiction to Prove a Case Is Not Possible.** Explore the statements in Parts (a) and (b) by considering several examples where the hypothesis is true.

(a) If an integer a is divisible by both 4 and 6, then it divisible by 24.
(b) If an integer a is divisible by both 2 and 3, then it divisible by 6.
(c) What can you conclude from the examples in Part (a)?
(d) What can you conclude from the examples in Part (b)?

The proof of the following proposition based on Part (b) uses cases. In this proof, however, we use cases and a proof by contradiction to prove that a certain integer cannot be odd. Hence, it must be even. Complete the proof of the proposition.

Proposition. Let $a \in \mathbb{Z}$. If 2 divides a and 3 divides a, then 6 divides a.

Proof : Let $a \in \mathbb{Z}$ and assume that 2 divides a and 3 divides a. We will prove that 6 divides a. Since 3 divides a, there exists an integer n such that

$$a = 3n. \tag{3.5.45}$$

The integer n is either even or it is odd. We will show that it must be even by obtaining a contradiction if it assumed to be odd. So, assume that n is odd. (Now complete the proof.)

23. **The Last Two Digits of a Large Integer.**
Notice that 7, 381, 272 $\equiv$ 72 (mod 100) since 7, 381, 272 - 72 = 7, 381, 200, which is divisible by 100. In general, if we start with an integer whose decimal representation has more than two digits and subtract the integer formed by the last two digits, the result will be an integer whose last two digits are 00. This result will be divisible by 100. Hence, any integer with more than 2 digits is congruent modulo 100 to the integer formed by its last two digits.

(a) Start by squaring both sides of the congruence $3^4 \equiv 81$ (mod 100) to prove that $3^8 \equiv 61$ (mod 100) and then prove that $3^{16} \equiv 21$ (mod 100). What does this tell you about the last two digits in the decimal representation of 3^{16}?
(b) Use the two congruences in Part (23a) and laws of exponents to determine r where $3^{20} \equiv r$ (mod 100) and $r \in \mathbb{Z}$ with $0 \le r < 100$. What does this tell you about the last two digits in the decimal representation of 3^{20}?
(c) Determine the last two digits in the decimal representation of 3^{400}.
(d) Determine the last two digits in the decimal representation of 4^{804}.
Hint: One way is to determine the "mod 100 values", for 4^2, 4^4, 4^8, 4^{16}, 4^{32}, 4^{64}, and so on. Then use these values and laws of exponents to determine r, where $4^{804} \equiv r$ (mod 100) and $r \in \mathbb{Z}$ with $0 \le r < 100$.
(e) Determine the last two digits in the decimal representation of 3^{3356}.
(f) Determine the last two digits in the decimal representation of 7^{403}.

Answer

Add texts here. Do not delete this text first.

This page titled 3.5: The Division Algorithm and Congruence is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

3.6: Review of Proof Methods

This section is different from others in the text. It is meant primarily as a review of the proof methods studied in Chapter 3. So the first part of the section will be a description of some of the main proof techniques introduced in Chapter 3. The most important part of this section is the set of exercises since these exercises will provide an opportunity to use the proof techniques that we have studied so far.

We will now give descriptions of three of the most common methods used to prove a conditional statement.

Direct Proof of a Conditional Statement $(P \to Q)$

- **When is it indicated?** This type of proof is often used when the hypothesis and the conclusion are both stated in a “positive” manner. That is, no negations are evident in the hypothesis and conclusion. That is, no negations are evident in the hypothesis and conclusion.
- **Description of the process.** Assume that P is true and use this to conclude that Q is true. That is, we use the forward-backward method and work forward from P and backward from Q.
- **Why the process makes sense.** We know that the conditional statement $P \to Q$ is automatically true when the hypothesis is false. Therefore, because our goal is to prove that $P \to Q$ is true, there is nothing to do in the case that P is false. Consequently, we may assume that P is true. Then, in order for $P \to Q$ to be true, the conclusion Q must also be true. (When P is true, but Q is false, $P \to Q$ is false.) Thus, we must use our assumption that P is true to show that Q is also true.

Proof of a Conditional Statement $(P \to Q)$ **Using the Contrapositive**

- **When is it indicated?** This type of proof is often used when both the hypothesis and the conclusion are stated in the form of negations. This often works well if the conclusion contains the operator “or”; that is, if the conclusion is in the form of a disjunction. In this case, the negation will be a conjunction.
- **Description of the process.** We prove the logically equivalent statement $\neg Q \to \neg P$. The forward-backward method is used to prove $\neg Q \to \neg P$. That is, we work forward from $\neg Q$ and backward from $\neg P$.
- **Why the process makes sense.** When we prove $\neg Q \to \neg P$, we are also proving $P \to Q$ because these two statements are logically equivalent. When we prove the contrapositive of $P \to Q$, we are doing a direct proof of $\neg Q \to \neg P$. So we assume $\neg Q$ because, when doing a direct proof, we assume the hypothesis, and $\neg Q$ is the hypothesis of the contrapositive. We must show $\neg P$ because it is the conclusion of the contrapositive.

Proof of $P \to Q$ **Using a Proof by Contradiction**

- When is it indicated? This type of proof is often used when the conclusion is stated in the form of a negation, but the hypothesis is not. This often works well if the conclusion contains the operator “or”; that is, if the conclusion is in the form of a disjunction. In this case, the negation will be a conjunction.
- Description of the process. Assume P and $\neg Q$ and work forward from these two assumptions until a contradiction is obtained.
- Why the process makes sense. The statement $P \to Q$ is either true or false. In a proof by contradiction, we show that it is true by eliminating the only other possibility (that it is false). We show that $P \to Q$ cannot be false by assuming it is false and reaching a contradiction. Since we assume that $P \to Q$ is false, and the only way for a conditional statement to be false is for its hypothesis to be true and its conclusion to be false, we assume that P is true and that Q is false (or, equivalently, that $\neg Q$ is true). When we reach a contradiction, we know that our original assumption that $P \to Q$ is false is incorrect. Hence, $P \to Q$ cannot be false, and so it must be true.

Other Methods of Proof

The methods of proof that were just described are three of the most common types of proof. However, we have seen other methods of proof and these are described below.

Proofs that Use a Logical Equivalency

As was indicated in Section 3.2, we can sometimes use of a logical equivalency to help prove a statement. For example, in order to prove a statement of the form

$$P \to (Q \vee R), \tag{3.6.1}$$

it is sometimes possible to use the logical equivalency

$$[P \to (Q \vee R)] \equiv [(P \wedge \neg Q) \to R]. \tag{3.6.2}$$

We would then prove the statement

$$[(P \wedge \neg Q) \to R]. \tag{3.6.3}$$

Most often, this would use a direct proof for statement (3.6.1) but other methods could also be used. Because of the logical equivalency, by proving statement (3.6.3), we have also proven the statement (3.6.1).

Proofs that Use Cases

When we are trying to prove a proposition or a theorem, we often run into the problem that there does not seem to be enough information to proceed. In this situation, we will sometimes use cases to provide additional assumptions for the forward process of the proof. When this is done, the original proposition is divided into a number of separate cases that are proven independently of each other. The cases must be chosen so that they exhaust all possibilities for the hypothesis of the original proposition. This method of case analysis is justified by the logical equivalency

$$(P \vee Q) \to R \equiv (P \to R) \wedge (Q \to R). \tag{3.6.4}$$

which was established in Preview Activity $3.6.1$ in Section 3.4.

Constructive Proof

This is a technique that is often used to prove a so-called existence theorem. The objective of an existence theorem is to prove that a certain mathematical object exists. That is, the goal is usually to prove a statement of the form

There exists an x such that $P(x)$.

For a constructive proof of such a proposition, we actually name, describe, or explain how to construct some object in the universe that makes $P(x)$ true.

Nonconstructive Proof

This is another type of proof that is often used to prove an existence theorem is the so-called **nonconstructive proof**. For this type of proof, we make an argument that an object in the universal set that makes $P(x)$ true must exist but we never construct or name the object that makes $P(x)$ true.

? Exercises for Section 3.6

1. Let h and k be real numbers and let r be a positive number. The equation for a circle whose center is at the point (h, k) and whose radius is r is

$$(x-h)^2 + (y-k)^2 = r^2. \tag{3.6.5}$$

We also know that if a and b are real numbers, then

- The point (a, b) is inside the circle if $(a-h)^2 + (b-k)^2 < r^2$.
- The point (a, b) is on the circle if $(a-h)^2 + (b-k)^2 = r^2$.
- The point (a, b) is outside the circle if $(a-h)^2 + (b-k)^2 > r^2$.

Prove that all points on or inside the circle whose equation is $(x-1)^2 + (y-2)^2 = 4$ are inside the circle whose equation is $x^2 + y^2 = 26$.

2. Let r be a positive real number. The equation for a circle of radius r whose center is the origin is $x^2 + y^2 = r^2$.

(a) Use implicit differentiation to determine $\frac{dy}{dx}$.
(b) Let (a, b) be a point on the circle with $a \neq 0$ and $b \neq 0$. Determine the slope of the line tangent to the circle at the point (a, b).
(c) Prove that the radius of the circle to the point (a, b) is perpendicular to the line tangent to the circle at the point (a, b).
Hint: Two lines (neither of which is horizontal) are perpendicular if and only if the products of their slopes is equal to 1.

3. Are the following statements true or false? Justify your conclusions.

(a) For each integer a, if 3 does not divide a, then 3 divides $2a^2 + 1$.

(b) For each integer a, if 3 divides $2a^2 + 1$, then 3 does not divide a.
(c) For each integer a, 3 does not divide a if and only if 3 divides $2a^2 + 1$.

4. Prove that for each real number x and each irrational number q, $x + q$ is irrational or $x - q$ is irrational.
5. Prove that there exist irrational numbers u and v such that uv is a rational number.

   Hint: We have proved that $\sqrt{2}$ is irrational. For the real number $q = \sqrt{2}^{\sqrt{2}}$, either q is rational or q is irrational. Use this disjunction to set up two cases.
6. Let a and b be natural numbers such that $a^2 = b^3$. Prove each of the propositions in Parts (6a) through (6d). (The results of Exercise (1) and Theorem 3.10 from Section 3.2 may be helpful.)

   (a) If a is even, then 4 divides a.
   (b) If 4 divides a, then 4 divides b.
   (c) If 4 divides b, then 8 divides a.
   (d) If a is even, then 8 divides a.
   (e) Give an example of natural numbers a and b such that a is even and $a^2 = b^3$, but b is not divisible by 8.
7. Prove the following proposition:
   Let a and b be integers with $a \leq 0$. If a does not divide b, then the equation $ax^3 + bx + (b + a) = 0$ does not have a solution that is a natural number.
   Hint: It may be necessary to factor a sum of cubes. Recall that

$$u^3 + v^3 = (u + v)(u^2 - uv + v^2). \tag{3.6.6}$$

8. Recall that a **Pythagorean triple** consists of three natural numbers a, b, and c such that $a < b < c$ and $a^2 + b^2 = c^2$. Are the following propositions true or false? Justify your conclusions.

   (a) For all $a, b, c \in \mathbb{N}$ such that $a < b < c$, if a, b, and c form a Pythagorean triple, then 3 divides a or 3 divides b.
   (b) For all $a, b, c \in \mathbb{N}$ such that $a < b < c$, if a, b, and c form a Pythagorean triple, then 5 divides a or 5 divides b or 5 divides c.
9. (a) Prove that there exists a Pythagorean triple a, b, and c, where $a = 5$ and b and c are consecutive natural numbers.
   (b) Prove that there exists a Pythagorean triple a, b, and c, where $a = 7$ and b and c are consecutive natural numbers.
   (c) Let m be an odd natural number that is greater than 1. Prove that there exists a Pythagorean triple a, b, and c, where $a = m$ and b and c are consecutive natural numbers.
10. One of the most famous unsolved problems in mathematics is a conjecture made by Christian Goldbach in a letter to Leonhard Euler in 1742. The conjecture made in this letter is now known as **Goldbach's Conjecture**. The conjecture is as follows:
    Every even integer greater than 2 can be expressed as the sum of two (not necessarily distinct) prime numbers.
    Currently, it is not known if this conjecture is true or false.

    (a) Write 50, 142, and 150 as a sum of two prime numbers
    (b)Prove the following:
    If Goldbach's Conjecture is true, then every integer greater than 5 can be written as a sum of three prime numbers.
    (c)Prove the following:
    If Goldbach's Conjecture is true, then every odd integer greater than 7 can be written as a sum of three odd prime numbers.
11. Two prime numbers that differ by 2 are called **twin primes**. For example, 3 and 5 are twin primes, 5 and 7 are twin primes, and 11 and 13 are twin primes. Determine at least two other pairs of twin primes. Is the following proposition true or false? Justify your conclusion.

    For all natural numbers p and q if p and q are twin primes other than 3 and 5, then $pq + 1$ is a perfect square and 36 divides $pq + 1$.
12. Are the following statements true or false? Justify your conclusions.

    (a) For all integers a and b, $(a + b)^2 \equiv (a^2 + b^2)(mod\ 2)$.
    (b) For all integers a and b, $(a + b)^3 \equiv (a^3 + b^3)(mod\ 3)$.
    (c) For all integers a and b, $(a + b)^4 \equiv (a^4 + b^4)(mod\ 4)$.

(d) For all integers a and b, $(a+b)^5 \equiv (a^5 + b^5)(mod\ 5)$.

If any of the statements above are false, write a new statement of the following form that is true (and prove that it is true):

For all integers a and b, $(a+b)^n \equiv (a^n + something + b^n)(mod n)$.

13. Let a, b, c, and d be real numbers with $a \neq 0$ and let $f(x) = ax^3 + bx^2 + cx + d$.

(a) Determine the derivative and second derivative of the cubic function f.

(b) Prove that the cubic function f has at most two critical points and has exactly one inflection point.

Explorations and Activities

14. **A Special Case of Fermat's Last Theorem**. We have already seen examples of **Pythagorean triples**, which are natural numbers a, b, and c where $a^2 + b^2 = c^2$. For example, 3, 4, and 5 form a Pythagorean triple as do 5, 12, and 13. One of the famous mathematicians of the 17th century was Pierre de Fermat (1601 – 1665). Fermat made an assertion that for each natural number n with $n \geq 3$, there are no integers a, b, and c for which $a^n + b^n = c^n$. This assertion was discovered in a margin of one of Fermat's books after his death, but Fermat provided no proof. He did, however, state that he had discovered truly remarkable proof but the margin did not contain enough room for the proof.

This assertion became known as **Fermat's Last Theorem** but it more prop- erly should have been called Fermat's Last Conjecture. Despite the efforts of mathematicians, this "theorem" remained unproved until Andrew Wiles, a British mathematician, first announced a proof in June of 1993. However, it was soon recognized that this proof had a serious gap, but a widely accepted version of the proof was published by Wiles in 1995. Wiles' proof uses many concepts and techniques that were unknown at the time of Fermat. We cannot discuss the proof here, but we will explore and prove the following proposition, which is a (very) special case of Fermat's Last Theorem.

Proposition. There do not exist prime numbers a, b,and c such that

$$a^3 + b3 = c3 \tag{3.6.7}$$

.

Although Fermat's Last Theorem implies this proposition is true, we will use a proof by contradiction to prove this proposition. For a proof by contradiction, we assume that

there exist prime numbers a, b, and c such that $a^3 + b^3 = c^3$.

Since 2 is the only even prime number, we will use the following cases: (1) $a = b = 2$; (2) a and b are both odd; and (3) one of a and b is odd and the other one is 2.

(a) Show that the case where $a = b = 2$ leads to a contradiction and hence, this case is not possible.
(b) Show that the case where a and b are both odd leads to a contradiction and hence, this case is not possible.
(c) We now know that one of a or b must be equal to 2. So we assume that $b = 2$ and that a is an odd prime. Substitute $b = 2$ into the equation $b^3 = c^3 - a^3$ and then factor the expression $c^3 - a^3$. Use this to obtain a contradiction.
(d) Write a complete proof of the proposition.

Answer

Add texts here. Do not delete this text first.

This page titled 3.6: Review of Proof Methods is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

3.S: Constructing and Writing Proofs in Mathematics (Summary)

Important Definitions

- Divides,divisor,page82
- Factor, multiple, page 82
- Proof, page 85
- Undefined term, page 85
- Axiom, page 85
- Definition,page86
- Conjecture, page 86
- Theorem, page 86
- Proposition,page 86
- Lemma, page 86
- Corollary, page 86
- Congruence modulo n, page 92
- Tautology,page 40
- Contradiction,page 40
- Absolutevalue,page 135

Important Theorems and Results about Even and Odd Integers

- **Exercise (1), Section 1.2**
  If m is an even integer, then $m+1$ is an odd integer.
  If m is an odd integer, then $m+1$ is an even integer.
- **Exercise (2), Section 1.2**
  If x is an even integer and y is an even integer, then $x+y$ is an even integer.
  If x is an even integer and y is an odd integer, then $x+y$ is an odd integer.
  If x is an odd integer and y is an odd integer, then $x+y$ is an even integer.
- **Exercise (3), Section 1.2.** *If x is an even integer and y is an integer, then $x \cdot y$ is an even integer.*
- **Theorem1.8.** *If x is an odd integer and y is an odd integer, then $x \cdot y$ is an odd integer.*
- **Theorem 3.7**. *The integer n is an even integer if and only if n^2 is an even integer.*
  Preview Activity $3.S.2$ in Section 3.2. *The integer n is an odd integer if and only if n^2 is an odd integer.*

Important Theorems and Results about Divisors

- **Theorem 3.1.** *For all integers a, b, and c with $a \neq 0$, if $a|b$ and $b|c$, then $a|c$.*
- **Exercise (3), Section 3.1**. *For all integers a, b, and c with $a \neq 0$,*
  If $a|b$ and $a|c$, then $a|(b+c)$.
  If $a|b$ and $a|c$, then $a|(b-c)$.
- **Exercise (3a), Section 3.1.** *For all integers a, b, and c with $a \neq 0$, if $a|b$, then $a|(bc)$.*
- **Exercise (4), Section 3.1.** *For all nonzero integers a and b, if $a|b$ and $b|a$, then $a = \pm b$.*

The Division Algorithm

Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that

$$a = bq + r \text{ and } 0 \leq r < b.$$

Important Theorems and Results about Congruence

- **Theorem 3.28.** *Let $a, b, c \in \mathbb{Z}$ and let $n \in \mathbb{N}$. If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then*

  $(a+c) \equiv (b+d) \pmod n$.

  $ac \equiv bd \pmod n$.
  For each $m \in \mathbb{N}$, $a^m \equiv b^m \pmod n$.

- **Theorem 3.30.** *For all integers a, b, and c,*
  Reflexive Property. $a \equiv a$ *(mod* n*).*
  Symmetric Property. *If* $a \equiv b$ *(mod* n*), then* $b \equiv a$ *(mod* n*).*
  Transitive Property. *If* $a \equiv b$ *(mod* n*) and* $b \equiv c$ *(mod* n*), then* $a \equiv c$ *(mod* n*).*
- **Theorem 3.31.** *Let* $a \in \mathbb{Z}$ *and let* $n \in \mathbb{N}$*. If* $a = nq + r$ *and* $0 \leq r < n$ *for some integers* q *and* r*, then* $a \equiv r$ *(mod* n*).*
- **Corollary 3.32.** *Each integer is congruent, modulo* n*, to precisely one of the integers 0, 1, 2, ...,* $n - 1$*. That is, for each integer* a*, there exists a unique integer* r *such that*

$$a \equiv r \text{ (mod } n) \text{ and } 0 \leq r < n.$$

This page titled 3.S: Constructing and Writing Proofs in Mathematics (Summary) is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

CHAPTER OVERVIEW

4: Mathematical Induction

Mathematical induction is a mathematical proof technique that is used to prove that a property $P(n)$ holds for every natural number n, i.e. for n = 0, 1, 2, 3, and so on.

4.1: The Principle of Mathematical Induction
4.2: Other Forms of Mathematical Induction
4.3: Induction and Recursion
4.S: Mathematical Induction (Summary)

Thumbnail: Mathematical induction can be informally illustrated by reference to the sequential effect of falling dominoes. Image used wtih permission (CC BY-SA 3.0; Pokipsy76).

This page titled 4: Mathematical Induction is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

4.1: The Principle of Mathematical Induction

Preview Activity $4.1.1$: Exploring Statements of the Form $(\forall n \in \mathbb{N})(P(n))$

One of the most fundamental sets in mathematics is the set of natural numbers $\mathbb{N}$. In this section, we will learn a new proof technique, called mathematical induction, that is often used to prove statements of the form $(\forall n \in \mathbb{N})(P(n))$. In Section 4.2, we will learn how to extend this method to statements of the form $(\forall n \in T)(P(n))$, where T is a certain type of subset of the integers $\mathbb{Z}$.

For each natural number n, let $P(n)$ be the following open sentence:

4 divides $(5^n - 1)$.

1. Does this open sentence become a true statement when $n = 1$? That is, is 1 in the truth set of $P(n)$?
2. Does this open sentence become a true statement when $n = 2$? That is, is 2 in the truth set of $P(n)$?
3. Choose at least four more natural numbers and determine whether the open sentence is true or false for each of your choices.

All of the examples that were used should provide evidence that the following proposition is true:

For each natural number n, 4 divides $(5^n - 1)$.

We should keep in mind that no matter how many examples we try, we cannot prove this proposition with a list of examples because we can never check if 4 divides $(5^n - 1)$ for every natural number n. Mathematical induction will provide a method for proving this proposition.

For another example, for each natural number n, we now let $Q(n)$ be the following open sentence:

$$1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{4.1.1}$$

The expression on the left side of the previous equation is the sum of the squares of the first n natural numbers. So when $n = 1$, the left side of equation (4.1.1) is 1^2. When $n = 2$, the left side of equation (4.1.1) is $1^2 + 2^2$.

4. Does $Q(n)$ become a true statement when
   - $n = 1$? (Is 1 in the truth set of $Q(n)$?
   - $n = 2$? (Is 1 in the truth set of $Q(n)$?
   - $n = 3$? (Is 1 in the truth set of $Q(n)$?
5. Choose at least four more natural numbers and determine whether the open sentence is true or false for each of your choices. A table with the columns n, $1^2 + 2^2 + ... + n^2$, and $\dfrac{n(n+1)(2n+1)}{6}$ may help you organize your work.

All of the examples we have explored, should indicate the following proposition is true:

For each natural number n, \(1^2 + 2^2 + ... + n^2 = \dfrac{n(n + 1)(2n + 1)}{6}.\]

In this section, we will learn how to use mathematical induction to prove this statement.

Preview Activity $4.1.1$: A Property of the Natural Numbers

Intuitively, the natural numbers begin with the number 1, and then there is 2, then 3, then 4, and so on. Does this process of "starting with 1" and "adding 1 repeatedly" result in all the natural numbers? We will use the concept of an inductive set to explore this idea in this activity.

Definition

A set T that is a subset of $\mathbb{Z}$ is an **inductive set** provided that for each integer k, if $k \in T$, then $k + 1 \in T$.

1. Carefully explain what it means to say that a subset T of the integers $\mathbb{Z}$ is not an inductive set. This description should use an existential quantifier.

2. Use the definition of an inductive set to determine which of the following sets are inductive sets and which are not. Do not worry about formal proofs, but if a set is not inductive, be sure to provide a specific counterexample that proves it is not inductive.

   (a) $A = \{1, 2, 3, ..., 20\}$
   (b) The set of natural numbers, $\mathbb{N}$
   (c) $B = \{n \in \mathbb{N} | n \geq 5\}$
   (d) $S = \{n \in \mathbb{Z} | n \geq -3\}$
   (e) $R = \{n \in \mathbb{Z} | n \leq 100\}$
   (f) The set of integers, $\mathbb{Z}$
   (g) The set of odd natural numbers.
3. This part will explore one of the underlying mathematical ideas for a proof by induction. Assume that $T \subseteq \mathbb{N}$ and assume that $1 \in T$ and that T is an inductive set. Use the definition of an inductive set to answer each of the following:

   (a) Is $2 \in T$? Explain.
   (b) Is $3 \in T$? Explain.
   (c) Is $4 \in T$? Explain.
   (d) Is $100 \in T$? Explain.
   (e) Do you think that $T = \mathbb{N}$? Explain.

Inductive Sets

The two open sentences in Preview Activity $4.1.1$ appeared to be true for all values of n in the set of natural numbers, $\mathbb{N}$. That is, the examples in this preview activity provided evidence that the following two statements are true.

- For each natural number n, 4 divides $(5^n - 1)$.
- For each natural number n, $1^2 + 2^2 + ... + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

One way of proving statements of this form uses the concept of an inductive set introduced in Preview Activity $4.1.2$. The idea is to prove that if one natural number makes the open sentence true, then the next one also makes the open sentence true. This is how we handle the phrase “and so on” when dealing with the natural numbers. In Preview Activity $4.1.2$, we saw that the number systems $\mathbb{N}$ and $\mathbb{Z}$ and other sets are inductive. What we are trying to do is somehow distinguish $\mathbb{N}$ from the other inductive sets. The way to do this was suggested in Part (3) of Preview Activity $4.1.2$. Although we will not prove it, the following statement should seem true.

Statement 1: For each subset T of $\mathbb{N}$, if $1 \in T$ and T is inductive, then $T = \mathbb{N}$.

Notice that the integers, $\mathbb{Z}$, and the set $S = \{n \in \mathbb{Z} | n \geq -3\}$ both contain 1 and both are inductive, but they both contain numbers other than natural numbers. For example, the following statement is false:

Statement 2: For each subset T of $\mathbb{Z}$, if $1 \in T$ and T is inductive, then $T = \mathbb{Z}$.

The set $S = \{n \in \mathbb{Z} | n \geq -3\} = \{-3, -2, -1, 0, 1, 2, 3, ...\}$ is a counterexample that shows that this statement is false.

? Progress Check 4.1 (Inductive Sets)

Suppose that T is an inductive subset of the integers. Which of the following statements are true, which are false, and for which ones is it not possible to tell?

1. $1 \in T$ and $5 \in T$.
2. If $1 \in T$, then $5 \in T$.
3. If $5 \notin T$, then $2 \notin T$.
4. For each integer k, if $k \in T$, then $k + 7 \in T$.
5. For each integer k, $k \notin T$ or $k + 1 \in T$.
6. There exists an integer k such that $k \in T$ and $k + 1 \notin T$.
7. For each integer k, if $k + 1 \in T$, then $k \in T$.
8. For each integer k, if $k + 1 \notin T$, then $k \notin T$.

Answer

Add texts here. Do not delete this text first.

The Principle of Mathematical Induction

Although we proved that Statement (2) is false, in this text, we will not prove that Statement (1) is true. One reason for this is that we really do not have a formal definition of the natural numbers. However, we should be convinced that Statement (1) is true. We resolve this by making Statement (1) an axiom for the natural numbers so that this becomes one of the defining characteristics of the natural numbers.

The Principle of Mathematical Induction

If T is a subset of $\mathbb{N}$ such that

1. $1 \in T$, and
2. For every $k \in \mathbb{N}$, if $k \in T$, then $(k+1) \in T$.

Then $T = \mathbb{N}$.

Using the Principle of Mathematical Induction

The primary use of the Principle of Mathematical Induction is to prove statements of the form

$$(\forall n \in \mathbb{N})(P(n)).$$

where $P(n)$ is some open sentence. Recall that a universally quantified statement like the preceding one is true if and only if the truth set T of the open sentence $P(n)$ is the set $\mathbb{N}$. So our goal is to prove that $T = \mathbb{N}$, which is the conclusion of the Principle of Mathematical Induction. To verify the hypothesis of the Principle of Mathematical Induction, we must

1. Prove that $1 \in T$. That is, prove that $P(1)$ is true.
2. Prove that if $k \in T$, then $(k+1) \in T$. That is, prove that if $P(k)$ is true, then $P(k+1)$ is true.

The first step is called the **basis step** or the **initial step**, and the second step is called the **inductive step**. This means that a proof by mathematical induction will have the following form:

Procedure for a Proof by Mathematical Induction

To prove: $(\forall n \in \mathbb{N})(P(n))$

Basis step: Prove $P(1)$.\

Inductive step: Prove that for each $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

We can then conclude that $P(n)$ is true for all $n \in \mathbb{N}$

Note that in the inductive step, we want to prove that the conditional statement "for each $k \in \mathbb{N}$, if $P(k)$ then $P(k+1)$" is true. So we will start the inductive step by assuming that $P(k)$ is true. This assumption is called the **inductive assumption** or the **inductive hypothesis**.

The key to constructing a proof by induction is to discover how $P(k+1)$ is related to $P(k)$ for an arbitrary natural number k. For example, in Preview Activity $4.1.1$, one of the open sentences $P(n)$ was

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Sometimes it helps to look at some specific examples such as $P(2)$ and $P(3)$. The idea is not just to do the computations, but to see how the statements are related. This can sometimes be done by writing the details instead of immediately doing computations.

$$P(2) \qquad is \qquad 1^2 + 2^2 = \frac{2 \cdot 3 \cdot 5}{6} \tag{4.1.2}$$

$$P(3) \qquad is \qquad 1^2 + 2^2 + 3^2 = \frac{3 \cdot 4 \cdot 7}{6} \tag{4.1.3}$$

In this case, the key is the left side of each equation. The left side of $P(3)$ is obtained from the left side of $P(2)$ by adding one term, which is 3^2. This suggests that we might be able to obtain the equation for $P(3)$ by adding 3^2 to both sides of the equation $P(2)$.

Now for the general case, if $k \in \mathbb{N}$, we look at $P(k+1)$ and compare it to $P(k)$.

$$P(k) \quad is \qquad 1^2 + 2^2 + \ldots + k^2 = \frac{k(k+1)(2k+1)}{6} \tag{4.1.4}$$

$$P(k+1) \quad is \quad 1^2 + 2^2 + \ldots + (k+1)^2 = \frac{(k+1)[(k+1)+1][2(k+1)+1]}{6} \tag{4.1.5}$$

The key is to look at the left side of the equation for $P(k+1)$ and realize what this notation means. It means that we are adding the squares of the first $k+1$ natural numbers. This means that we can write

$$1^2 + 2^2 + \ldots + (k+1)^2 = 1^2 + 2^2 + \ldots + k^2 + (k+1)^2.$$

This shows us that the left side of the equation for $P(k+1)$ can be obtained from the left side of the equation for $P(k)$ by adding $(k+1)^2$. This is the motivation for proving the inductive step in the following proof.

Proposition 4.2.

For each natural number n,

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Proof

We will use a proof by mathematical induction. For each natural number n, we let $P(n)$ be

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

We first prove that $P(1)$ is true. Notice that $\dfrac{1(1+1)(2 \cdot 1 + 1)}{6} = 1$. This shows that

\(1^2 = \dfrac{1(1 + 1)(2 \cdot 1 + 1}{6},

which proves that $P(1)$ is true.

For the inductive step, we prove that for each $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true. So let k be a natural number and assume that $P(k)$ is true. That is, assume that

$$1^2 + 2^2 + \ldots + k^2 = \frac{k(k+1)(2k+1)}{6}. \tag{4.1.6}$$

The goal now is to prove that $P(k+1)$ is true. That is, it must be proved that

$$\begin{align} 1^2 + 2^2 + \ldots + k^2 + (k+1)^2 &= \frac{(k+1)[(k+1)+1][2(k+1)+1]}{6} \tag{4.1.7} \\ &= \frac{(k+1)(k+2)(2k+3)}{6}. \tag{4.1.8} \end{align}$$

To do this, we add $(k+1)^2$ to both sides of equation (1) and algebraically rewrite the right side of the resulting equation. This gives

$$\begin{align} 1^2 + 2^2 + \ldots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \tag{4.1.9} \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \tag{4.1.10} \\ &= \frac{(k+1)[k(2k+1) + 6(k+1)]}{6} \tag{4.1.11} \\ &= \frac{(k+1)(2k^2 + 7k + 6)}{6} \tag{4.1.12} \\ &= \frac{(k+1)(k+2)(2k+3) + 6(k+1)^2}{6} \tag{4.1.13} \end{align}$$

Comparing this result to equation (2), we see that if $P(k)$ is true, then $P(k+1)$ is true. Hence, the inductive step has been established, and by the Principle of Mathematical Induction, we have proved that for each natural number n, $1^2 + 2^2 + \ldots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

Writing Guideline

The proof of Proposition 4.2 shows a standard way to write an induction proof. When writing a proof by mathematical induction, we should follow the guideline that we always keep the reader informed. This means that at the beginning of the proof, we should state that a proof by induction will be used. We should then clearly define the open sentence (P(n)\) that will be used in the proof.

Summation Notation

The result in Proposition 4.2 could be written using summation notation as follows:

$$\text{For each natural number } n, \sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}.$$

In this case, we use j for the index for the summation, and the notation $\sum_{j=1}^{n} j^2$ tells us to add all the values of j^2 for j from 1 to n, inclusive. That is,

$$\sum_{j=1}^{n} j^2 = 1^2 + 2^2 + \ldots + n^2.$$

So in the proof of Proposition 4.2, we would let $P(n)$ be $\sum_{j=1}^{n} j^2 = \dfrac{n(n+1)(2n+1)}{6}$, and we would use the fact that for each natural number k,

$$\sum_{j=1}^{k+1} j^2 = (\sum_{j=1}^{k} j^2) + (k+1)^2.$$

? Progress Check 4.3 (An Example of a Proof by Induction)

1. Calculate $1+2+3+\ldots+n$ and $\dfrac{n(n+1)}{2}$ for several natural numbers n. What do you observe?
2. Use mathematical induction to prove that $1+2+3+\ldots+n = \dfrac{n(n+1)}{2}$. To do this, let $P(n)$ be the open sentence, "$1+2+3+\ldots+n = \dfrac{n(n+1)}{2}$." For the basis step, notice that the equation $1 = \dfrac{1(1+1)}{2}$ shows that $P(1)$ is true. Now let k be a natural number and assume that $P(k)$ is true. That is, assume that

$$1+2+3+\ldots+k = \frac{k(k+1)}{2}, \tag{4.1.14}$$

   and complete the proof.

Answer

Add texts here. Do not delete this text first.

Some Comments about Mathematical Induction

1. The basis step is an essential part of a proof by induction. See Exercise (19) for an example that shows that the basis step is needed in a proof by induction.
2. Exercise (20) provides an example that shows the inductive step is also an essential part of a proof by mathematical induction.
3. It is important to remember that the inductive step in an induction proof is a proof of a conditional statement. Although we did not explicitly use the forward-backward process in the inductive step for Proposition 4.2, it was implicitly used in the discussion prior to Proposition 4.2. The key question was, “How does knowing the sum of the first k squares help us find the sum of the first $(k+1)$ squares?”
4. When proving the inductive step in a proof by induction, the key question is,

   How does knowing $P(k)$ help us prove $P(k+1)$?

   In Proposition 4.2, we were able to see that the way to answer this question was to add a certain expression to both sides of the equation given in $P(k)$. Sometimes the relationship between $P(k)$ and $P(k+1)$ is not as easy to see. For example, in Preview

Activity $4.1.1$, we explored the following proposition:

For each natural number n, 4 divides $(5^n - 1)$.

This means that the open sentence, $P(n)$, is "4 divides $(5^n - 1)$." So in the inductive step, we assume $k \in \mathbb{N}$ and that 4 divides $(5^k - 1)$. This means that there exists an integer m such that

$$5^k - 1 = 4m. \tag{4.1.15}$$

In the backward process, the goal is to prove that 4 divides $(5^{k+1} - 1)$. This can accomplished if we can prove that there exists an integer s such that

$$5^{k+1} - 1 = 4s. \tag{4.1.16}$$

We now need to see if there is anything in equation (4.1.15) that can be used in equation (4.1.16). The key is to find something in the equation $5^k - 1 = 4m$ that is related to something similar in the equation $5^{k+1} - 1 = 4s$ In this case, we notice that

$$5^{k+1} = 5 \cdot 5^k. \tag{4.1.17}$$

So if we can solve $5^k - 1 = 4m$ for 5^k, we could make a substitution for 5^k. This is done in the proof of the following proposition. page195image4184747072

Proposition 4.4.

For every natural number n, 4 divides $(5^n - 1)$.

Proof

(Proof by Mathematical Induction) For each natural number n, let $P(n)$ be "4 divides $(5^n - 1)$" We first prove that $P(1)$ is true. Notice that when $n = 1$, $5^n - 1 = 4$. Since 4 divides 4, $P(1)$ is true.

For the inductive step, we prove that for all $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true. So let k be a natural number and assume that $P(k)$ is true. That is, assume that

$$4 \text{ divides } (5^k - 1).$$

This means that there exists an integer m such that

$$5^k - 1 = 4m.$$

Thus,

$$5^k = 4m + 1. \tag{4.1.18}$$

In order to prove that $P(k+1)$ is true, we must show that 4 divides $(5^{k+1} - 1)$. Since $5^{k+1} = 5 \cdot 5^k$, we can write

$$5^{k+1} - 1 = 5 \cdot 5^k - 1. \tag{4.1.19}$$

We now substitute the expression for 5k from equation (4.1.18) into equation (4.1.19). This gives

$$\begin{aligned} 5^{k+1} - 1 &= 5 \cdot 5^k - 1 \\ &= 5(4m+1) - 1 \\ &= (20m+5) - 1 \\ &= 20m + 4 \\ &= 4(5m+1) \end{aligned} \tag{4.1.20}$$

Since $(5m+1)$ is an integer, equation (4.1.20) shows that 4 divides $(5^{k+1} - 1)$. Therefore, if $P(k)$ is true, then $P(k+1)$ is true and the inductive step has been established. Thus, by the principle of Mathematical Induction, for every natural number n, 4 divides $(5^n - 1)$.

Proposition 4.4 was stated in terms of “divides.” We can use congruence to state a proposition that is equivalent to Proposition 4.4. The idea is that the sentence, 4 divides $(5^n - 1)$ means that $5^n \equiv 1$ (mod 4). So the following proposition is equivalent to Proposition 4.4.

Proposition 4.5.

For every natural number n, $5^n \equiv 1$ (mod 4).

Since we have proved Proposition 4.4, we have in effect proved Proposition 4.5. However, we could have proved Proposition 4.5 first by using the results in Theorem 3.28 on page 147. This will be done in the next progress check.

Progress Check 4.6 (Proof of Proposition 4.5) .

To prove Proposition 4.5, we let $P(n)$ be $5^n \equiv 1$ (mod 4) and notice that $P(1)$ is true since $5 \equiv 1$ (mod 4). For the inductive step, let k be a natural number and assume that $P(k)$ is true. That is, assume that $5^n \equiv 1$ (mod 4).

1. What must be proved in order to prove that $P(k+1)$ is true?
2. Since $5^{k+1} = 5 \cdot 5^k$, multiply both sides of the congruence $5^k \equiv 1$ (mod 4) by 5. The results in Theorem 3.28 on page 147 justify this step.
3. Now complete the proof that for each $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true and complete the induction proof of Proposition 4.5.

It might be nice to compare the proofs of Propositions 4.4 and 4.5 and decide which one is easier to understand.

Answer

Add texts here. Do not delete this text first.

Exercises for Section 4.1

1. Which of the following sets are inductive sets? Explain.

   (a) $\mathbb{Z}$
   (b) $\{x \in \mathbb{N} | x \geq 4\}$
   (c) $\{x \in \mathbb{Z} | x \leq 10\}$
   (d) {1, 2, 3, ..., 500}
2. (a) Can a finite, nonempty set be inductive? Explain.
   (b) Is the empty set inductive? Explain.
3. Use mathematical induction to prove each of the following:

   (a) For each natural number n, $2 + 5 + 8 + \cdots + (3n-1) = \dfrac{n(3n+1)}{2}$.
   (b) For each natural number n, $1 + 5 + 9 + \cdots + (4n-3) = n(2n-1)$.
   (c) For each natural number n, $1^3 + 2^3 + 3^3 + \cdots + n^3 = [\dfrac{n(n+1)}{2}]^2$.
4. Based on the results in Progress Check 4.3 and Exercise (3c), if $n \in \mathbb{N}$, is there any conclusion that can be made about the relationship between the sum $(1^3 + 2^3 + 3^3 + ... + n^3)$ and the sum $(1 + 2 + 3 + \cdots + n)$?
5. Instead of using induction, we can sometimes use previously proven results about a summation to obtain results about a different summation.

   (a) Use the result in Progress Check4.3 to prove the following proposition:

   $$\text{For each natural number } n, 3 + 6 + 9 + ... + 3n = \frac{3n(n+1)}{2}. \tag{4.1.21}$$

   (b) Subtract n from each side of the equation in Part (a). On the left side of this equation, explain why this can be done by subtracting 1 from each term in the summation.

(c) Algebraically simplify the right side of the equation in Part (b) to obtain a formula for the sum $2+5+8+...(3n-1)$. Compare this to Exercise (3a).

6. (a) Calculate $1+3+5+\cdots+(2n-1)$ for several nuatural numbers n.
   (b) Based on your work in exercise (6a), if $n\in\mathbb{N}$, make a conjecture about the value of the sum $1+3+5+\cdots+(2n-1) = \sum_{j=1}^{n}(2j-1)$.
   (c) Use mathematical induction to prove your conjecture in Exercise (6b).
7. In Section 3.1, we defined congruence modulo n for a natural number n, and in Section 3.5, we used the Division Algorithm to prove that each integer is congruent, modulo n, to precisely one of the integers 0, 1, 2, \cdot\cdot\cdot, $n-1$(Corollary 3.32).

   (a) Find the value of r so that $4\equiv r$ (mod 3) and $r\in\{0,1,2\}$.
   (b) Find the value of r so that $4^2\equiv r$ (mod 3) and $r\in\{0,1,2\}$.
   (c) Find the value of r so that $4^3\equiv r$ (mod 3) and $r\in\{0,1,2\}$.
   (d) For two other values of n, find the value of r so that $4^n\equiv r$ (mod 3) and $r\in\{0,1,2\}$.
   (e) If $n\in\mathbb{N}$ make a conjecture concerning the value of r where $4^n\equiv r$ (mod 3) and $r\in\{0,1,2\}$. This conjecture should be written as a self-contained proposition including an appropriate quantifier.
   (f) Use mathematical induction to prove your conjecture.
8. Use mathematical induction to prove each of the following:

   (a) For each natural number n, 3 divides (4^n-1).
   (b) For each natural number n, 6 divides (n^3-n).
9. In Exercise (7), we proved that for each natural number n, $4^n\equiv 1$ (mod 3). Explain how this result is related to the proposition in Exercise (8a).
10. Use mathematical induction to prove that for each natural number n, 3 divides n^3+23n. Compare this proof to the proof from Exercise (18) in Section 3.5.
11. (a) Calculate the value of 5^n-2^n for $n=1, n=2, n=3, n=4, n=5$ and $n=6$.
    (b) Based on your work in Part (a), make a conjecture about the values of 5^n-2^n for each natural number n.
    (c) Use mathematical induction to prove your conjecture in Part (b).
12. Let x and y be integers. Prove that for each natural number n, $(x-y)$ divides (x^n-y^n). Explain why your conjecture in Exercise (11) is a special case of this result.
13. Prove Part (3) of Theorem 3.28 from Section 3.4. Let $n\in\mathbb{N}$ and let a and b be integers. For each $m\in\mathbb{N}$, if $a\equiv b$ (mod n), then $a^m\equiv b^m$ (mod n).
14. Use mathematical induction to prove that the sum of the cubes of any three consecutive natural numbers is a multiple of 9.
15. Let a be a real number. We will explore the derivatives of the function $f(x)=e^{ax}$. By using the chain rule, we see that

$$\frac{d}{dx}(e^{ax}) = ae^{ax}. \tag{4.1.22}$$

    Recall that the second derivative of a function is the derivative of the derivative function. Similarly, the third derivative is the derivative of the second derivative.

    (a) What is $\frac{d^2}{dx^2}(e^{ax})$, the second derivative of e^{ax}?
    (b) What is $\frac{d^3}{dx^3}(e^{ax})$, the third derivative of e^{ax}?
    (c) Let n be a natural number. Make a conjecture about the nth derivatives of the function $f(x)=e^{ax}$. That is, what is $\frac{d^n}{dx^n}(e^{ax})$? This conjecture should be written as a self-contained proposition including an appropriate quantifier.
    (d) Use mathematical induction to prove that your conjecture.
16. In calculus, it can be shown that

$$\begin{aligned} \int sin^2xdx &= \frac{x}{2}-\frac{1}{2}sinxcosx+c \quad \text{and} \\ \int cos^2xdx &= \frac{x}{2}+\frac{1}{2}sinxcosx+c. \end{aligned} \tag{4.1.23}$$

Using integration by parts, it is also possible to prove that for each natural number n,

$$\begin{aligned}\int sin^n x dx &= -\frac{1}{n} sin^{n-1} x cos x + \frac{n-1}{n}\int sin^{n-2} x dx \quad \text{and}\\ \int cos^n x dx &= \frac{1}{n} cos^{n-1} x sin x + \frac{n-1}{n}\int cos^{n-2} x dx.\end{aligned} \tag{4.1.24}$$

(a) Determine the values of

$$\int_0^{\pi/2} sin^2 x dx \quad \text{and} \quad \int_0^{\pi/2} sin^4 x dx. \tag{4.1.25}$$

(b) Use mathematical induction to prove that for each natural number n

$$\begin{aligned}\int_0^{\pi/2} sin^{2n} x dx &= \frac{1\cdot3\cdot5\cdots(2n-1)}{2\cdot4\cdot6\cdots(2n)}\frac{\pi}{2} \quad \text{and}\\ \int_0^{\pi/2} sin^{2n+1} x dx &= \frac{2\cdot4\cdot6\cdots(2n)}{1\cdot3\cdot5\cdots(2n+1)}.\end{aligned} \tag{4.1.26}$$

These are known as the ***Wallis sine formulas***.
(c) Use mathematical induction to prove that

$$\begin{aligned}\int_0^{\pi/2} cos^{2n} x dx &= \frac{1\cdot3\cdot5\cdots(2n-1)}{2\cdot4\cdot6\cdots(2n)}\frac{\pi}{2} \quad \text{and}\\ \int_0^{\pi/2} cos^{2n+1} x dx &= \frac{2\cdot4\cdot6\cdots(2n)}{1\cdot3\cdot5\cdots(2n+1)}.\end{aligned} \tag{4.1.27}$$

These are known as the ***Wallis cosine formulas***.

17. (a) Why is it not possible to use mathematical induction to prove a proposition of the form

$$(\forall x \in \mathbb{Q})(P(x)), \tag{4.1.28}$$

where $P(x)$ is some predicate?
(b) Why is it not possible to use mathematical induction to prove a proposition of the form
For each real number x with $x \geq 1$, $P(x)$,
where \(P(x) is some predicate?

18. **Evaluation of proofs**
See the instructions for Exercise (19) on page 100 from Section 3.1.

(a)

For each natural number n, $1+4+7+\cdots+(3n-2) = \dfrac{n(3n-1)}{2}$.

Proof

We will prove this proposition using mathematical induction. So we let $P(n)$ be the open sentence

$$1+4+7+\cdots+(3n-2).$$

Using $n=1$, we see taht $3n-2=1$ and hence, $P(1)$ is true.

We now assume taht $P(k)$ is true. That is,

$$1+4+7+\cdots+(3k-2) = \frac{k(3k-1)}{2}.$$

We then see that

$$\begin{aligned} 1+4+7+\cdots+(3k-2)+(3(k+1)-2) &= \frac{(k+1)(3k+2)}{2} \\ \frac{k(3k-1)}{2}+(3k+1) &= \frac{(k+1)(3k+2)}{2} \\ \frac{(3k^2-k)+(6k+2)}{2} &= \frac{3k^2+5k+2}{2} \\ \frac{3k^2+5k+2}{2} &= \frac{3k^2+5k+2}{2}. \end{aligned} \tag{4.1.29}$$

We have thus proved that $P(k+1)$ is true, and hence, we have proved the proposition.

(b)

For each natural number n, $1+4+7+\cdots+(3n-2) = \dfrac{n(3n-1)}{2}$.

Proof

We will prove this proposition using mathematical induction. So we let

$$P(n) = 1+4+7+\cdots+(3n-2).$$

Using $n=1$, we see that $P(1)=1$ and hence, $P(1)$ is true.

We now assume that $P(k)$ is true. That is,

$$1+4+7+\cdots+(3k-2) = \frac{k(3k-1)}{2}.$$

We then see that

$$\begin{aligned} P(k+1) &= 1+4+7+\cdots+(3k-2)+(3(k+1)-2) \\ &= \frac{k(3k-2)}{2}+3(k+1)-2 \\ &= \frac{3k^2-k+6k+6-4}{2} \\ &= \frac{3k^2+5k+2}{2} \\ &= \frac{(k+1)(3k+2)}{2}. \end{aligned} \tag{4.1.30}$$

we have thus proved that $P(k+1)$ is true, and hence, we have proved the proposition.

(c)

All dogs are the same breed.

Proof

We will prove this proposition using mathematical induction. For each natural number n, we let $P(n)$ be

Any set of n dogs consists entirely of dogs of the same breed.

We will prove that for each natural number n, $P(n)$ is true, which will prove that all dogs are the same breed. A set with only one dog consists entirely of dogs of the same breed and, hence, $P(1)$ is true.

So we let k be a natural number and assume that $P(k)$ is true, that is, that every set of k dogs consists of dogs of the same breed. Now consider a set D of $k+1$ dogs, where

$$D = \{d_1, d_2, \ldots, d_k, d_{k+1}\}.$$

If we remove the dog d_1 from the set D, we then have a set D_1 of k dogs, and using the assumption that $P(k)$ is true, these dogs must all be of the same breed. Similarly, if we remove d_{k+1} from the set D, we again have a set D_2 of k

dogs, and these dogs must all be of the same breed. Since $D = D_1 \cup D_2$, we have proved that all of the dogs in D must be of the same breed.

This proves that if $P(k)$ is true, then $P(k+1)$ is true and, hence, by mathematical induction, we have proved that for each natural number n, any set of n dogs consists entirely of dogs of the same breed.

Explorations and Activities

19. **The Importance of the Basis Step**. Most of the work done in constructing a proof by induction is usually in proving the inductive step. This was certainly the case in Proposition 4.2. However, the basis step is an essential part of the proof. Without it, the proof is incomplete. To see this, let $P(n)$ be

$$1 + 2 + \cdots + n = \frac{n^2 + n + 1}{2}. \tag{4.1.31}$$

(a) Let $k \in \mathbb{N}$. Complete the following proof that if $P(k)$ is true, then $P(k+1)$ is true.
Let $k \in mathbbN$. Assume that $P(k)$ is true. That is, assume that

$$1 + 2 + \cdots + k = \frac{k^2 + k + 1}{2}. \tag{4.1.32}$$

The goal is to prove that $P(k+1)$ is true. That is, we need to prove that

$$1 + 2 + \cdots + k + (k+1) = \frac{(k+1)^2 + (k+1) + 1}{2}. \tag{4.1.33}$$

To do this, we add $k+1$ to both sides of equation (4.1.32). This gives

$$\begin{aligned} 1 + 2 + \cdots + k + (k+1) &= \frac{k^2 + k + 1}{2} + (k+1) \\ &= \cdots. \end{aligned} \tag{4.1.34}$$

(b) Is $P(1)$ true? Is $P(2)$ true? What about $P(3)$ and $P(4)$? Explain how this shows that the basis step is an essential part of a proof by induction.

20. **Regions of a Circle.** Place n equally spaced points on a circle and connect each pair of points with the chord of the circle determined by that pair of points. See Figure 4.1.

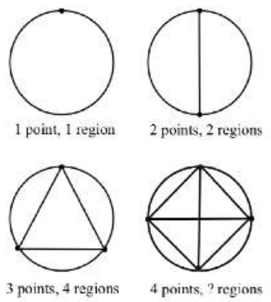


Figure 4.1: Regions of Circles

Count the number of distinct regions within each circle. For example, with three points on the circle, there are four distinct regions. Organize your data in a table with two columns: “Number of Points on the Circle” and “Number of Distinct Regions in the Circle.”

(a) How many regions are there when there are four equally spaced points on the circle?
(b) Based on the work so far, make a conjecture about how many distinct regions would you get with five equally spaced

points.

(c) Based on the work so far, make a conjecture about how many distinct regions would you get with six equally spaced points.

(d) Figure 4.2 shows the figures associated with Parts (b) and (c). Count the number of regions in each case. Are your conjectures correct or incorrect?

(e) Explain why this activity shows that the inductive step is an essential part of a proof by mathematical induction.

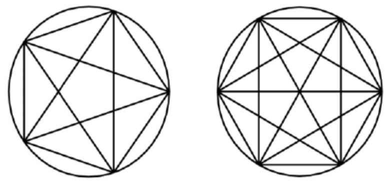


Figure 4.2: Regions of Circles

Answer

Add texts here. Do not delete this text first.

This page titled 4.1: The Principle of Mathematical Induction is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

4.2: Other Forms of Mathematical Induction

? Preview Activity 4.2.1: Exploring a Proposition about Factorials

Definition

If n is a natural number, we define n *factorial*, denoted by $n!$, to be the product of the first n natural numbers. In addition, we define $0!$ to be equal to 1.

Using this definition, we see that

$$\begin{array}{lllllll} 0! & = & 1 & \qquad & 3! & = & 1\cdot 2\cdot 3 = 6 \\ 1! & = & 1 & & 4! & = & 1\cdot 2\cdot 3\cdot 4 = 24 \\ 2! & = & 1\cdot 2 = 2 & & 5! & = & 1\cdot 2\cdot 3\cdot 4\cdot 5 = 120. \end{array} \tag{4.2.1}$$

In general, we write $n! = 1\cdot 2\cdot 3\cdots(n-1)\cdot n$ or $n! = n\cdot(n-1)\cdots 2\cdot 1$. Notice that for any natural number n, $n! = n\cdot(n-1)!$.

1. Compute the values of 2^n and $n!$ for each natural number n with $1 \leq n \leq 7$.

Now let $P(n)$ be the open sentence, "$n! > 2^n$."

2. Which of the statements $P(1)$ through $P(1)$ are true?

3. Based on the evidence so far, does the following proposition appear to be true or false? For each natural number n with $n \geq 4$, $n! > 2^n$.

Let k be a natural number with $k \geq 4$. Suppose that we want to prove that if $P(k)$ is true, then $P(k+1)$ is true. (This could be the inductive step in an induction proof.) To do this, we would be assuming that $k! > 2^k$ and would need to prove that $(k+1)! > 2^{k+1}$. Notice that if we multiply both sides of the inequality $k! > 2^k$ by $(k+1)$, we obtain

$$(k+1)\cdot k! > (k+1)2^k. \tag{4.2.2}$$

4. In the inequality in (4.2.2), explain why $(k+1)\cdot k! = (k+1)!$.

5. Now look at the right side of the inequality in (4.2.2). Since we are assuming that $k \geq 4$, we can conclude that $(k+1) > 2$. Use this to help explain why $(k+1)2^k > 2^{k+1}$.

6. Now use the inequality in (4.2.2) and the work in steps (4) and (5) to explain why $(k+1)! > 2^{k+1}$.

? PREVIEW ACTIVITY 4.2.1: Prime Factors of a Natural Number

Recall that a natural number p is a **prime number** provided that it is greater than 1 and the only natural numbers that divide p are 1 and p. A natural number other than 1 that is not a prime number is a **composite number**. The number 1 is neither prime nor composite.

1. Give examples of four natural numbers that are prime and four natural numbers that are composite.
2. Write each of the natural numbers 20, 40, 50, and 150 as a product of prime numbers.
3. Do you think that any composite number can be written as a product of prime numbers?
4. Write a useful description of what it means to say that a natural number is a composite number (other than saying that it is not prime).
5. Based on your work in Part (2), do you think it would be possible to use induction to prove that any composite number can be written as a product of prime numbers?

The Domino Theory

Mathematical induction is frequently used to prove statements of the form

$$(\forall n \in \mathbb{N})(P(n)). \tag{4.2.3}$$

where $P(n)$ is an open sentence. This means that we are proving that every statement in the following infinite list is true.

$$P(1),\ P(2),\ P(3) \tag{4.2.4}$$

$$P(1), P(2), P(3), \ldots \tag{4.2.4}$$

The inductive step in a proof by induction is to prove that if one statement in this infinite list of statements is true, then the next statement in the list must be true. Now imagine that each statement in Equation ??? is a domino in a chain of dominoes. When we prove the inductive step, we are proving that if one domino is knocked over, then it will knock over the next one in the chain. Even if the dominoes are set up so that when one falls, the next one will fall, no dominoes will fall unless we start by knocking one over. This is why we need the basis step in an induction proof. The basis step guarantees that we knock over the first domino. The inductive step, then, guarantees that all dominoes after the first one will also fall.

Now think about what would happen if instead of knocking over the first domino, we knock over the sixth domino. If we also prove the inductive step, then we would know that every domino after the sixth domino would also fall. This is the idea of the *Extended Principle of Mathematical Induction*. It is not necessary for the basis step to be the proof that $P(1)$ is true. We can make the basis step be the proof that $P(M)$ is true, where M is some natural number. The Extended Principle of Mathematical Induction can be generalized somewhat by allowing M to be any integer. We are still only concerned with those integers that are greater than or equal to M.

The Extended Principle of Mathematical Induction

Let M be an integer. If T is a subset of $\mathbb{Z}$ such that

1. $M \in T$, and
2. For every $k \in \mathbb{Z}$ with $k \geq M$, if $k \in T$, then $(k+1) \in T$,

Then T contains all integers greater than or equal to M. That is $\{n \in \mathbb{Z} | n \geq M\} \subseteq T$.

Using the Extended Principle of Mathematical Induction

The primary use of the Principle of Mathematical Induction is to prove statements of the form

$$(\forall n \in \mathbb{Z}, \text{ with} n \geq M)(P(n)).$$

where M is an integer and $P(n)$ is some open sentence. (In most induction proofs, we will use a value of M that is greater than or equal to zero.) So our goal is to prove that the truth set T of the predicate $P(n)$ contains all integers greater than or equal to M. So to verify the hypothesis of the Extended Principle of Mathematical Induction, we must

1. Prove that $M \in T$, That is, prove that $P(M)$ is true.
2. Prove that for every $k \in \mathbb{Z}$ with $k \geq M$, if $k \in T$, then $(k+1) \in T.\text{Thatis},$ prove that if $P(k)$ is true, then $P(k+1)$ is true.

As before, the first step is called the **basis step** or the **initial step**, and the second step is called the **inductive step**. This means that a proof using the Extended Principle of Mathematical Induction will have the following form:

Using the Extended Principle of Mathematical Induction

Let M be an integer. To prove: $(\forall n \in \mathbb{Z}, \text{ with} n \geq M)(P(n))$.

Basis step: Prove $P(M)$.

Inductive step: Prove that for every $k \in \mathbb{Z}$ with $k \geq M$, if $P(k)$ is true, then $P(k+1)$ is true.

We can then conclude that $P(n)$ is true for all $n \in \mathbb{Z}, \text{ with} n \geq M)(P(n))$.

This is basically the same procedure as the one for using the Principle of Mathematical Induction. The only difference is that the basis step uses an integer M other than 1. For this reason, when we write a proof that uses the Extended Principle of Mathematical Induction, we often simply say we are going to use a proof by mathematical induction. We will use the work from Preview Activity $4.2.1$ to illustrate such a proof.

Proposition 4.7

For each natural number n with $n \geq 4$, $n! > 2^n$.

Proof

We will use a proof by mathematical induction. For this proof, we let

$P(n)$ be "$n! > 2^n$."

We first prove that $P(4)$ is true. Using $n = 4$, we see that $4! = 24$ and $2^4 = 16$. This means that $4! > 2^4$ and, hence, $P(4)$ is true.

For the inductive step, we prove that for all $k \in \mathbb{N}$ with $k \geq 4$, if $P(k)$ is true, then $P(k+1)$ is true. So let k be a natural number greater than or equal to 4, and assume that $P(k)$ is true. That is, assume that

$$k! > 2^k. \tag{4.2.5}$$

The goal is to prove that $P(k+1)$ is true or that $(k+1)! > 2^{k+1}$. Multiplying both sides of inequality (4.2.5) by $k+1$ gives

$$\begin{array}{rcl} (k+1) \cdot k! & > & (k+1) \cdot 2^k, \text{ or} \\ (k+1)! & > & (k+1) \cdot 2^k. \end{array} \tag{4.2.6}$$

Now $k \geq 4$. Thus, $k+1 > 2$, and hence $(k+1) \cdot 2^k > 2 \cdot 2^k$. This means that

$$(k+1) \cdot 2^k > 2^{k+1}. \tag{4.2.7}$$

Inequalities (4.2.6) and (4.2.7) show that

$$(k+1)! > 2^{k+1}.$$

and this proves that if $P(k)$ is true, then $P(k+1)$ is true. Thus, the inductive step has been established, and so by the Extended Principle of Mathematical Induction, $n! > 2^n$ for each natural number n with $n \geq 4$.

? Progress Check 4.8: Formulating Conjectures

Formulate a conjecture (with an appropriate quantifier) that can be used as an an- swer to each of the following questions.

1. For which natural numbers n is 3^n greater than $1 + 2^n$?
2. For which natural numbers n is 2^n greater than \((n + 1)^2)?
3. For which natural numbers n is $(1 + \frac{1}{n})^n$ less than n ?

Answer

Add texts here. Do not delete this text first.

The Second Principle of Mathematical Induction

Let $P(n)$ be

n is a prime number or n is a product of prime numbers.

(This is related to the work in Preview Activity $4.2.2$.)

Suppose we would like to use induction to prove that $P(n)$ is true for all natural numbers greater than 1. We have seen that the idea of the inductive step in a proof by induction is to prove that if one statement in an infinite list of statements is true, then the next statement must also be true. The problem here is that when we factor a composite number, we do not get to the previous case. For example, if assume that P.39/ is true and we want to prove that $P(40)$ is true, we could factor 40 as $40 = 2 \cdot 20$. However, the assumption that $P(39)$ is true does not help us prove that $P(40)$ is true.

This work is intended to show the need for another principle of induction. In the inductive step of a proof by induction, we assume one statement is true and prove the next one is true. The idea of this new principle is to assume that all of the previous statements are true and use this assumption to prove the next statement is true. This is stated formally in terms of subsets of natural numbers in the Second Principle of Mathematical Induction. Rather than stating this principle in two versions, we will state the extended version of the Second Principle. In many cases, we will use $M = 1$ or $M = 0$.

The Second Principle of Mathematical Induction

Let M be an integer. If T is a subset of $\mathbb{Z}$ such that

1. $M \in T$, and
2. For every $k \in \mathbb{Z}$ with $k \geq M$, if $\{M, M+1, \ldots, k\} \subseteq T$, then $(k+1) \in T$.

Then T contains all integers greater than or equal to M. That is $\{n \in \mathbb{Z} | n \geq M\} \subseteq T$.

Using the Second Principle of Mathematical Induction

The primary use of mathematical induction is to prove statements of the form

$(\forall n \in \mathbb{Z},\ \text{with} n \geq M)(P(n))$,

where M is an integer and $P(n)$ is some predicate. So our goal is to prove that the truth set T of the predicate $P(n)$ contains all integers greater than or equal to M. To use the Second Principle of Mathematical Induction, we must

1. Prove that $M \in T$, That is, prove that $P(M)$ is true.
2. Prove that for every $k \in \mathbb{N}$, if $k \geq M$ and $\{M, M+1, \ldots, k\} \subseteq T$, then $(k+1) \in T$. That is, prove that if $P(M)$, $P(M+1)$, ..., $P(k)$ are true, then $P(k+1)$ is true.

As before, the first step is called the **basis step** or the **initial step**, and the second step is called the **inductive step**. This means that a proof using the Second Principle of Mathematical Induction will have the following form:

Using the Second Principle of Mathematical Induction

Let M be an integer. To prove: $\forall n \in \mathbb{Z} \text{with} n \geq M)(P(n))$

Basis step: Prove $P(M)$.

Inductive step: Let $k \in \mathbb{Z}$ with $k \geq M$. Prove that if $P(M)$, $P(M+1)$, ..., $P(k)$ are true, then $P(k+1)$ is true.

We can then conclude that $P(n)$ is true for all $n \in \mathbb{Z}$ with $n \geq M$.

We will use this procedure to prove the proposition suggested in Preview Activity $4.2.2$.

Theorem 4.9

Each natural number greater than 1 is either a prime number or is a product of prime numbers.

Proof

We will use the Second Principle of Mathematical Induction. We let $P(n)$ be

n is either a prime number or n is a product of prime numbers.

For the basis step, $P(2)$ is true since 2 is a prime number.

To prove the inductive step, we let k be a natural number with $k \geq 2$. We assume that $P(2)$, $P(3)$, ..., $P(k)$ are true. That is, we assume that each of the natural numbers 2, 3, ..., k is a prime number or a product of prime numbers. The goal is to prove that $P(k+1)$ is true or that $(k+1)$ is a prime number or a product of prime numbers.

Case 1: If $(k+1)$ is a prime number, then $P(k+1)$ is true.

Case 2: If $(k+1)$ is not a prime number, then $(k+1)$ can be factored into a product of natural numbers with each one being less than $(k+1)$. That is, there exist natural numbers a and b with

$k+1 = a \cdot b$, and $1 < a \leq k$ and $1 < b \leq k$.

Using the inductive assumption, this means that $P(a)$ and $P(b)$ are both true. Consequently, a and b are prime numbers or are products of prime numbers. Since $k+1 = a \cdot b$, we conclude that $(k+1)$ is a product of prime numbers. That is, we conclude that $P(k+1)$ is true. This proves the inductive step.

Hence, by the Second Principle of Mathematical Induction, we conclude that $P(n)$ is true for all $n \in \mathbb{N}$ with $n \geq 2$, and this means that each natural number greater than 1 is either a prime number or is a product of prime numbers.

We will conclude this section with a progress check that is really more of an activity. We do this rather than including the activity at the end of the exercises since this activity illustrates a use of the Second Principle of Mathematical Induction in which it is convenient to have the basis step consist of the proof of more than one statement.

Progress Check 4.10 (Using the Second Principle of Induction)

Consider the following question:

For which natural numbers n do there exist nonnegative integers x and $y$such that $n = 3x + 5y$?

To help answer this question, we will let $\mathbb{Z}^* = \{x \in \mathbb{Z} | x \ge 0\}$, and let $P(n)$ be

$$\text{There exist } x, y \in \mathbb{Z}^* \text{ such that } n = 3x + 5y.$$

Notice that $P(1)$ is false since if both x and y are zero, then $3x + 5y = 0$ and if either $x > 0$ or $y > 0$, then $3x + 5y \ge 3$. Also notice that $P(6)$ is true since $6 = 3 \cdot 2 + 5 \cdot 0$ and $P(8)$ is true since $8 = 3 \cdot 1 + 5 \cdot 1$.

1. Explain why $P(2)$, $P(4)$, and $P(7)$ are false and why $P(3)$ and $P(5)$ are true.
2. Explain why $P(9)$, $P(10)$, $P(11)$, and $P(12)$ are true.

We could continue trying to determine other values of n for which $P(n)$ is true. However, let us see if we can use the work in part (2) to determine if $P(13)$ is true. Notice that $13 = 3 + 10$ and we know that $P(10)$ is true. We should be able to use this to prove that $P(13)$ is true. This is formalized in the next part.

3. Let $k \in \mathbb{N}$. Prove that if $P(8)$, $P(9)$, ..., $P(k)$ are true, then $P(k+1)$ is true. **Hint:** $k + 1 = 3 + (k - 2)$.

4. Prove the following proposition using mathematical induction. Use the Sec- ond Principle of Induction and have the basis step be a proof that $P(8)$, $P(9)$, and $P(10)$ are true. (The inductive step is part (3).)

Proposition 4.11.

For each $n \in \mathbb{N}$ with $n \ge 8$, there exist nonnegative integers x and y such that $n = 3x + 5y$.

Answer

Add texts here. Do not delete this text first.

Exercises for Section 4.2

1. Use mathematical induction to prove each of the following:

   (a) For each natural number n with $n \ge 2$, $3^n > 1 + 2^n$.
   (b) For each natural number n with $n \ge 6$, $2^n > (n+1)^2$.
   (c) For each natural number n with $n \ge 3$, $(1 + \frac{1}{n})^n < n$.
2. For each natural number n with $n^2 < 2^n$? Justify your conclusion.
3. For each natural number n with $n! > 3^n$? Justify your conclusion.
4. (a) Verify that $(1 - \frac{1}{4}) = \frac{3}{4}$ and that $(1 - \frac{1}{4})(1 - \frac{1}{9}) = \frac{4}{6}$.
   (b) Verify that $(1 - \frac{1}{4})(1 - \frac{1}{9})(1 - \frac{1}{16}) = \frac{5}{8}$ and that $(1 - \frac{1}{4})(1 - \frac{1}{9})(1 - \frac{1}{16})(1 - \frac{1}{25}) = \frac{6}{10}$.
   (c) For $n \in \mathbb{N}$ with $n \ge 2$, make a conjecture about a formula for the product $(1 - \frac{1}{4})(1 - \frac{1}{9})(1 - \frac{1}{16}) \cdots (1 - \frac{1}{n^2})$.
   (d) Based on your work in Parts (4a) and (4b), state a. proposition and then use the Extended Principle of Mathematical Induction to prove your proposition.
5. Is the following proposition true or false? Justify your conclusion.
   For each nonnegative integer n, $8^n | (4n)!$:
6. Let $y = lnx$.

   (a) Determine $\frac{dy}{dx}$, $\frac{d^2y}{dx^2}$, $\frac{d^3y}{dx^3}$, and $\frac{d^4y}{dx^4}$.

(b) Let n be a natural number. Formulate a conjecture for a formula for $\frac{d^n y}{dx^n}$. Then use mathematical induction to prove your conjecture.

7. For which natural numbers n do there exist nonnegative integers x and y such that $n = 4x + 5y$? Justify your conclusion.
8. Can each natural number greater than or equal to 4 be written as the sum of at least two natural numbers, each of which is a 2 or a 3? Justify your conclusion. For example, $7 = 2 + 2 + 3$, and $17 = 2 + 2 + 2 + 2 + 3 + 3 + 3$.
9. Can each natural number greater than or equal to 6 be written as the sum of at least two natural numbers, each of which is a 2 or a 5? Justify your conclusion. For example, $6 = 2 + 2 + 2$, $9 = 2 + 2 + 5$, and $17 = 2 + 5 + 5 + 5$.
10. Use mathematical induction to prove the following proposition:

    Let x be a real number with $x > 0$. Then for each natural number n with $n \geq 2$, $(1 + x)^n > 1 + nx$.

    Explain where the assumption that $x > 0$ was used in the proof.
11. Prove that for each odd natural number n with $n \geq 3$,

$$(1 + \frac{1}{2})(1 - \frac{1}{3})(1 + \frac{1}{4}) \cdots (1 + \frac{(-1)^n}{n}) = 1. \tag{4.2.8}$$

12. Prove that for each natural number n,

    any set. with n elements has $\frac{n(n-1)}{2}$ two-element subsets.
13. Prove or disprove each of the following propositions:

    (a) For each $n \in \mathbb{N}$, $\frac{1}{1 \cdot 2}. + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$.
    (b) For each natural number n with $n \geq 3$,

$$\frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} + \cdots + \frac{1}{n(n+1)} = \frac{n-2}{3n+3} \tag{4.2.9}$$

    .
    (c) For each $n \in \mathbb{N}$, $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$.
14. Is the following proposition true or false? Justify your conclusion.

    For each natural number n, $(\frac{n^3}{3} + \frac{n^2}{2} + \frac{7n}{6})$ is a natural number.
15. Is the following proposition true or false? Justify your conclusion.

    For each natural number n, $(\frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30})$ is an integer.
16. (a) Prove that if $n \in \mathbb{N}$, then there exists an odd natural number m and a nonnegative integer k such that $n = 2^k m$.
    (b) For each $n \in \mathbb{N}$, prove that there is only one way to write n in the form described in Part (a). To do this, assume that $n = 2^k m$ and $n = 2^q p$ where m and p are odd natural numbers and k and q are nonnegative integers. Then prove that $k = q$ and $m = p$.
17. Evaluation of proofs
    See the instructions for Exercise (19) on page 100 from Section 3.1.

(a)

For each natural number n with $n \geq 2$, $2^n > 1 + n$.

Proof

We let k be a natural number and assume that $2^k > 1 + k$. Multiplying both sides of this inequality by 2, we see that $2^{k+1} > 2 + 2k$. However, $2 + 2k > 2 + k$ and, hence,

$$2^{k+1} > 1 + (k + 1).$$

By mathematical induction, we conclude that $2^n > 1 + n$.

(b)

Each natural number greater than or equal to 6 can be written as the sum of natural numbers, each of which is a 2 or a 5.

Proof

We will use a proof by induction. For each natural number n, we let $P(n)$ be, "There exist nonnegative integers x and y such that $n = 2x + 5y$." Since

$$\begin{array}{rclcrcl} 6 & = & 3 \cdot 2 + 0 \cdot 5 & & 7 & = & 2 + 5 \\ 8 & = & 4 \cdot 2 + 0 \cdot 5 & & 9 & = & 2 \cdot 2 + 1 \cdot 5 \end{array} \tag{4.2.10}$$

We see that $P(6)$, $P(7)$, $P(8)$, and $P(9)$ are true.

We now suppose that for some natural number k with $k \geq 10$ that $P(6)$, $P(7)$, ... $P(k)$ are true. Now

$$k + 1 = (k - 4) + 5.$$

Since $k \geq 10$, we see that $k - 4 \geq 6$ and, hence, $P(k - 4)$ is true. So $k - 4 = 2x + 5y$ and, hence,

$$\begin{array}{rcl} k + 1 & = & (2x + 5y) + 5 \\ & = & 2x + 5(y + 1). \end{array} \tag{4.2.11}$$

This proves that $P(k + 1)$ is true, and hence, by the Second Principle of Mathematical Induction, we have proved that for each natural number n with $n \geq 6$, there exist nonnegative integers x and y such that $n = 2x + 5y$.

Explorations and Activities

18. **The Sum of the Angles of a Convex Quadrilateral.** There is a famous theorem in Euclidean geometry that states that the sum of the interior angles of a triangle is 180°.

    (a) Use the theorem about triangles to determine the sum of the angles of a convex quadrilateral. **Hint:** Draw a convex quadrilateral and draw a diagonal.
    (b) Use the result in Part (1) to determine the sum of the angles of a convex pentagon.
    (c) Use the result in Part (2) to determine the sum of the angles of a convex hexagon.
    (d) Let n be a natural number with $n \geq 3$. Make a conjecture about the sum of the angles of a convex polygon with n sides and use mathematical induction to prove your conjecture.
19. **De Moivre's Theorem**. One of the most interesting results in trigonometry is De Moivre's Theorem, which relates the complex number i to the trigonometric functions. Recall that the number i is the complex number whose square is 1, that is, $i^2 = -1$. One version of the theorem can be stated as follows:
    If x is a real number, then for each nonnegative integer n.

    $$[cos x + i(sin x)]^n = cos(nx) + i(sin(nx)). \tag{4.2.12}$$

    This theorem is named after Abraham de Moivre (1667 – 1754), a French mathematician.

    (a) The proof of De Moivre's Theorem requires the use of the trigonometric identities for the sine and cosine of the sum of two angles. Use the Internet or a book to find identities for $sin(\alpha + \beta)$ and $cos(\alpha + \beta)$.
    (b) To get a sense of how things work, expand $[cos x + i(sin x)]^2$ and write the result in the form $a + bi$. Then use the identities from part (1) to prove that $[cos x + i(sin x)]^2 = cos(2x) + i(sin(2x))$.
20. (c) Use mathematical induction to prove De Moivre's Theorem.

Answer

Add texts here. Do not delete this text first.

This page titled 4.2: Other Forms of Mathematical Induction is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

4.3: Induction and Recursion

Preview Activity $4.3.1$: Recursively Defined Sequences

In a proof by mathematical induction, we “start with a first step” and then prove that we can always go from one step to the next step. We can use this same idea to define a sequence as well. We can think of a **sequence** as an infinite list of numbers that are indexed by the natural numbers (or some infinite subset of $\mathbb{N} \cup \{0\}$). We often write a sequence in the following form:

$$a_1, a_2, ..., a_n, ...$$

The number a_n is called the n^{th} term of the sequence. One way to define a sequence is to give a specific formula for the n^{th} term of the sequence such as $a_n = \dfrac{1}{n}$.

Another way to define a sequence is to give a specific definition of the first term (or the first few terms) and then state, in general terms, how to determine a_{n+1} in terms of n and the first n terms $a_1, a_2, ..., a_n$. This process is known as **definition by recursion** and is also called a **recursive definition**. The specific definition of the first term is called the **initial condition**, and the general definition of a_{n+1} in terms of n and the first n terms $a_1, a_2, ..., a_n$ is called the recurrence relation. (When more than one term is defined explicitly, we say that these are the initial conditions.) For example, we can define a sequence recursively as follows:

$b_1 = 16$, and for each $n \in \mathbb{N}$, $b_{n+1} = \dfrac{1}{2}b_n$.

Using $n = 1$ and then $n = 2$, we then see that

Missing argument for b column declaration

1. Calculate b_4 through b_{10}. What seems to be happening to the values of b_n as n gets larger?
2. Define a sequence recursively as follows:
   $T_1 = 16$, and for each $n \in \mathbb{N}$, $T_{n+1} = 16 + \dfrac{1}{2}T_n$.

   Then $T_2 = 16 + \dfrac{1}{2}T_1 = 16 + 8 = 24$. Caluculate T_3 through T_{10}. What seems to be happening to the values of T_n as n gets larger?

The sequences in Parts (1) and (2) can be generalized as follows: Let a and r be real numbers. Define two sequences recursively as follows:

$a_1 = a$, and for each $n \in \mathbb{N}$, $a_{n+1} = r \cdot a_n$.

$S_1 = a$, and for each $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$.

3. Determine formulas (in terms of a and r) for a_2 through a_6. What do you think an is equal to (in terms of a, r, and n)?
4. Determine formulas (in terms of a and r) for S_2 through S_6. What do you think an is equal to (in terms of a, r, and n)?

   In Preview Activity $4.3.1$ in Section 4.2, for each natural number n, we defined $n!$, read n **factorial**, as the product of the first n natural numbers. We also defined $0!$ to be equal to 1. Now recursively define a sequence of numbers a_0, a_1, a_2, ... as follows:

   $a_0 = 1$, and
   for each nonnegative integer n, $a_{n+1} = (n+1) \cdot a_n$.

   Using $n = 0$, we see that this implies that $a_1 = 1 \cdot a_0 = 1 \cdot 1 = 1$, Then using $n = 1$, we see that

$$a_2 = 2a_1 = 2 \cdot 1 = 2. \tag{4.3.1}$$

5. Calculate a_3, a_4, a_5 and a_6.
6. Do you think that it is possible to calculate a_{20} and a_{100}? Explain.
7. Do you think it is possible to calculate a_n for any natural number n? Explain.

8. Compare the values of a_0, a_1, a_2, a_3, a_4, a_5, and a_6 with those of 0!, 1!, 2!, 3!, 4!, 5!, and 6!. What do you observe? We will use mathematical induction to prove a result about this sequence in Exercise (1).

✓ Preview Activity 4.3.1: The Fibonacci Numbers

The Fibonacci numbers are a sequence of natural numbers f_1, f_2, f_3, ..., f_n, ... defined recursively as follows:

- $f_1 = 1$ and $f_2 = 1$, and
- For each natural number n, $f_{n+2} = f_{n+1} + f_n$.

In words, the recursion formula states that for any natural number n with $n \geq 3$, the n^{th} Fibonacci number is the sum of the two previous Fibonacci numbers. So we see that

Illegal pream-token (f)

1. Calculate f_6 through f_{20}.
2. Which of the Fibonacci numbers f_1 through f_{20} are even? Which are multiples of 3?
3. For $n = 2$, $n = 3$, $n = 4$, and $n = 5$, how is the sum of the first $(n-1)$ Fibonacci numbers related to the $(n+1)^{st}$ Fibonacci number?
4. Record any other observations about the values of the Fibonacci numbers or any patterns that you observe in the sequence of Fibonacci numbers. If necessary, compute more Fibonacci numbers.

The Fibonacci Numbers

The Fibonacci numbers form a famous sequence in mathematics that was investigated by Leonardo of Pisa (1170 – 1250), who is better known as Fibonacci. Fibonacci introduced this sequence to the Western world as a solution of the following problem:

> *Suppose that a pair of adult rabbits (one male, one female) produces a pair of rabbits (one male, one female) each month. Also, suppose that newborn rabbits become adults in two months and produce another pair of rabbits. Starting with one adult pair of rabbits, how many pairs of rabbits will be produced each month for one year?*

Since we start with one adult pair, there will be one pair produced the first month, and since there is still only one adult pair, one pair will also be produced in the second month (since the new pair produced in the first month is not yet mature). In the third month, two pairs will be produced, one by the original pair and one by the pair which was produced in the first month. In the fourth month, three pairs will be produced, and in the fifth month, five pairs will be produced.

The basic rule is that in a given month after the first two months, the number of adult pairs is the number of adult pairs one month ago plus the number of pairs born two months ago. This is summarized in Table 4.1, where the number of pairs produced is equal to the number of adult pairs, and the number of adult pairs follows the Fibonacci sequence of numbers that we developed in Preview Activity 4.3.2.

Table 4.1: Fibonacci Numbers

Months	1	2	3	4	5	6	7	8	9	10
Adult Pairs	1	1	2	3	5	8	13	21	34	55
Newborn Pairs	1	1	2	3	5	8	13	21	34	55
Month-Old Pairs	0	1	1	2	3	5	8	13	21	34

Historically, it is interesting to note that Indian mathematicians were studying these types of numerical sequences well before Fibonacci. In particular, about fifty years before Fibonacci introduced his sequence, Acharya Hemachandra (1089 – 1173) considered the following problem, which is from the biography of Hemachandra in the *MacTutor History of Mathematics Archive:*

> Suppose we assume that lines are composed of syllables which are either short or long. Suppose also that each long syllable takes twice as long to articulate as a short syllable. A line of length n contains n units where each short syllable is one unit

> and each long syllable is two units. Clearly a line of length n units takes the same time to articulate regardless of how it is composed. Hemchandra asks: How many different combinations of short and long syllables are possible in a line of length n?

This is an important problem in the Sanskrit language since Sanskrit meters are based on duration rather than on accent as in the English Language. The answer to this question generates a sequence similar to the Fibonacci sequence. Suppose that hn is the number of patterns of syllables of length n. We then see that $h_1 = 1$ and $h_2 = 2$. Now let n be a natural number and consider pattern of length $n + 2$. This pattern either ends in a short syllable or a long syllable. If it ends in a short syllable and this syllable is removed, then there is a pattern of length $n + 1$, and there are $h_n + 1$ such patterns. Similarly, if it ends in a long syllable and this syllable is removed, then there is a pattern of length n, and there are h_n such patterns. From this, we conclude that

$$h_{n+2} = h_{n+1} + h_n.$$

This actually generates the sequence 1, 2, 3, 5, 8, 13, 21, ... For more information about Hemachandra, see the article *Math for Poets and Drummers* by Rachel Wells Hall in the February 2008 issue of *Math Horizons*.

We will continue to use the Fibonacci sequence in this book. This sequence may not seem all that important or interesting. However, it turns out that this sequence occurs in nature frequently and has applications in computer science. There is even a scholarly journal, *The Fibonacci Quarterly*, devoted to the Fibonacci numbers.

The sequence of Fibonacci numbers is one of the most studied sequences in mathematics, due mainly to the many beautiful patterns it contains. Perhaps one observation you made in Preview Activity $4.3.2$ is that every third Fibonacci number is even. This can be written as a proposition as follows:

For each natural number n, f_{3n} is an even natural number.

As with many propositions associated with definitions by recursion, we can prove this using mathematical induction. The first step is to define the appropriate open sentence. For this, we can let $P(n)$ be, "f_{3n} is an even natural number."

Notice that $P(1)$ is true since $f_{3n} = 2$. We now need to prove the inductive step. To do this, we need to prove that for each $k \in \mathbb{N}$,

if $P(k)$ is true, then $P(k + 1)$ is true.

That is, we need to prove that for each $k \in \mathbb{N}$, if f_{3k} is even, then $f_{3(k+1)}$ is even.

So let's analyze this conditional statement using a know-show table.

Step	Know	Reason
P	f_{3k} is even	Inductive hypothesis
$P1$	$(\exists m \in \mathbb{N})(f_{3k} = 2m)$	Definition of "even integer"
...	...	...
$Q1$	$(\exists q \in \mathbb{N})(f_{3(k+1)} = 2q)$	
Q	$f_{3(k+1)}$ is even.	Definition of "even integer"
Step	**Show**	**Reason**

The key question now is, "Is there any relation between $f_{3(k+1)}$ and f_k?" We can use the recursion formula that defines the Fibonacci sequence to find such a relation.

The recurrence relation for the Fibonacci sequence states that a Fibonacci number (except for the first two) is equal to the sum of the two previous Fibonacci numbers. If we write $3(k + 1) = 3k + 3$, then we get $f_{3(k+1)} = f_{3k+3}$. For f_{3k+3}, the two previous Fibonacci numbers are f_{3k+2} and f_{3k+1}. This means that

$$f_{3k+3} = f_{3k+2} + f_{3k+1}.$$

Using this and continuing to use the Fibonacci relation, we obtain the following:

$$\begin{aligned} f_{3(k+1)} &= f_{3k+3} \\ &= f_{3k+2} + f_{3k+1} \\ &= (f_{3k+1} + f_{3k}) + f_{3k+1}. \end{aligned} \tag{4.3.2}$$

The preceding equation states that $f_{3(k+1)} = 2f_{3k+1} + f_{3k}$. This equation can be used to complete the proof of the induction step.

Progress Check 4.12 (Every Third Fibonacci Number Is Even)

Complete the proof of Proposition 4.13.

Proposition 4.13.

For each natural number n, the Fibonacci number f_{3n} is an even natural number.

Hint: We have already defined the predicate $P(n)$ to be used in an induction proof and have proved the basis step. Use the information in and after the preceding know-show table to help prove that if f_{3k} is even, then $f_{3(k+1)}$ is even.

Answer

Add texts here. Do not delete this text first.

Geometric Sequences and Geometric Series

Let $a,\ r \in \mathbb{R}$. The following sequence was introduced in Preview Activity $4.3.1$.

$$\begin{array}{rcl}\text{Initial condition} & : & a_1 = a. \\ \text{Recurrence relation} & : & \text{For each } n \in \mathbb{N}, a_{n+1} = r \cdot a_n.\end{array} \tag{4.3.3}$$

This is a recursive definition for a **geometric sequence** with **initial term** a and (common) **ratio** r. The basic idea is that the next term in the sequence is obtained by multiplying the previous term by the ratio r. The work in Preview Activity $4.3.1$ suggests that the following proposition is true.

Theorem 4.14

Let $a,\ r \in \mathbb{R}$, If a geometric sequence is defined by $a_1 = a$ and for each $n \in \mathbb{N}$, $a_{n+1} = r \cdot a_n$, then for each $n \in \mathbb{N}$, $a_n = a \cdot r^{n-1}$.

Proof

The proof of this proposition is Exercise (6).

Another sequence that was introduced in Preview Activity $4.3.1$ is related to geometric series and is defined as follows:

$$\begin{array}{rcl}\text{Initial condition} & : & S_1 = a. \\ \text{Recurrence relation} & : & \text{For each } n \in \mathbb{N}, S_{n+1} = r \cdot S_n.\end{array} \tag{4.3.4}$$

For each $n \in \mathbb{N}$, the term S_n is a (finite) **geometric series** with **initial term** a and (common) **ratio** r. The work in Preview Activity $4.3.1$ suggests that the following proposition is true.

Theorem 4.15

Let $a,\ r \in \mathbb{R}$. If the sequence $S_1, S_2, \ldots, S_n, \ldots$ is defined by $S_1 = a$ and for each $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$, then for each $n \in \mathbb{N}$, $S_n = a + a \cdot r + a \cdot r^2 + \cdots + a \cdot r^{n-1}$. That is, the geometric series S_n is the sum of the first n terms of the corresponding geometric sequence.

Proof

Add proof here and it will automatically be hidden if you have a "AutoNum" template active on the page.

The proof of Proposition 4.15 is Exercise (7). The recursive definition of a geometric series and Proposition 4.15 give two different ways to look at geometric series. Proposition 4.15 represents a geometric series as the sum of the first nterms of the corresponding geometric sequence. Another way to determine this sum a geometric series is given in Theorem 4.16, which gives a formula for the sum of a geometric series that does not use a summation.

Theorem 4.16

Let $a, \ r \in \mathbb{R}$ *and* $r \neq 1$*. If the sequence* $S_1, S_2, ..., S_n, ...$ *is defined by* $S_1 = a$ *and for each* $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$*, then for each* $n \in \mathbb{N}$, $S_n = a(\dfrac{1 - r^n}{1 - r})$.

Proof

The proof of Proposition 4.16 is Exercise (8).

Exercises for Section 4.3

1. For the sequence $a_0, a_1, a_2, ..., a_n, ...$, assume that $a_0 = 1$ and that for each $n \in \mathbb{N} \cup \{0\}$, $a_{n+1} = (n+1)a_n$. Use mathematical induction to prove that for each $n \in \mathbb{N} \cup \{0\}$, $a_n = n!$.
2. Assume that $f_1, f_2, ..., f_n, ...$ are the Fibonacci numbers. Prove each of the following:

   (a) For each $n \in \mathbb{N}$, f_{4n} is a multiple of 3.
   (b) For each $n \in \mathbb{N}$, f_{5n} is a multiple of 5.
   (c) For each $n \in \mathbb{N}$, with $n \geq 2$, $f_1 + f_2 + \cdots + f_{n-1} = f_{n+1} - 1$.
   (d) For each $n \in \mathbb{N}$, $f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$.
   (e) For each $n \in \mathbb{N}$, $f_2 + f_4 + \cdots + f_{2n} = f_{2n+1} - 1$.
   (f) For each $n \in \mathbb{N}$, $f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}$.
   (g) For each $n \in \mathbb{N}$ such that $n \not\equiv 0 \pmod 3$, f_n is an odd integer.
3. Use the result in Part (f) of Exercise (2) to prove that

$$\frac{f_1^2 + f_2^2 + \cdots + f_n^2 + f_{n+1}^2}{f_1^2 + f_2^2 + \cdots + f_n^2} = 1 + \frac{f_{n+1}}{f_n} \tag{4.3.5}$$

4. The quadratic formula can be used to show that $\alpha = \dfrac{1 + \sqrt{5}}{2}$ and $\beta = \dfrac{1 - \sqrt{5}}{2}$ are the two real number solutions of the quadratic equation $x^2 - x - 1 = 0$. Notice that this implies that

$$\begin{aligned} \alpha^2 &= \alpha + 1, \text{ and} \\ \beta^2 &= \beta + 1. \end{aligned} \tag{4.3.6}$$

   It may be surprising to find out that these two irrational numbers are closely related to the Fibonacci numbers.

   (a) Verify that $f_1 = \dfrac{\alpha^1 - \beta^1}{\alpha - \beta}$ and that $f_2 = \dfrac{\alpha^2 - \beta^2}{\alpha - \beta}$
   (b) (This part is optional, but it may help with the induction proof in part (c).) Work with the relation $f_3 = f_2 + f_1$ and substitute the expressions for f_1 and f_2 from part (a). Rewrite the expression as a single fraction and then in the numerator use $\alpha^2 + \alpha = \alpha(\alpha + 1)$ and a similar equation involving β. Now prove that $f_3 = \dfrac{\alpha^3 - \beta^3}{\alpha - \beta}$.
   (c) Use induction to prove that for each natural number n, if $\alpha = \dfrac{1 + \sqrt{5}}{2}$ and $\beta = \dfrac{1 - \sqrt{5}}{2}$, then $f_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$. **Note**: This formula for the n^{th} Fibonacci number is known as Binet's formula, named after the French mathematician Jacques Binet (1786 - 1856).
5. Is the following conjecture true or false? Justify your conclusion.

   Conjecture. Let $f_1, f_2, ..., f_m, ...$ be the sequence of the Fibonacci numbers. For each natural number n, the numbers $f_n f_{n+3}$, $2f_{n+1}f_{n+2}$, and $(f_{n+1}^2 + f_{n+2}^2)$ form a Pythagorean triple.
6. Prove Proposition 4.14. Let $a, \ r \in \mathbb{R}$, If a geometric sequence is defined by $a_1 = a$ and for each $n \in \mathbb{N}$, $a_{n+1} = r \cdot a_n$, then for each $n \in \mathbb{N}$, $a_n = a \cdot r^{n-1}$.
7. Prove Proposition 4.15. Let $a, \ r \in \mathbb{R}$. If the sequence $S_1, S_2, ..., S_n, ...$ is defined by $S_1 = a$ and for each $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$, then for each $n \in \mathbb{N}$, $S_n = a + a \cdot r + a \cdot r^2 + \cdots + a \cdot r^{n-1}$. That is, the geometric series S_n is the sum of the first n terms of the corresponding geometric sequence.

8. Prove Proposition 4.16. Let $a,\ r \in \mathbb{R}$ and $r \neq 1$. If the sequence $S_1, S_2, \ldots, S_n, \ldots$ is defined by $S_1 = a$ and for each $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$, then for each $n \in \mathbb{N}$, $S_n = a(\dfrac{1-r^n}{1-r})$.
9. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 2$ and that for each $n \in \mathbb{N}$, $a_{n+1} = a_n + 5$.

   (a) Calculate a_2 through a_6.
   (b) Make a conjecture for a formula for a_n for each n for each $n \in \mathbb{N}$.
   (c) Prove that your conjecture in Exercise (9b) is correct.
10. The sequence in Exercise (9) is an example of an **arithmetic sequence.** An arithmetic sequence is defined recursively as follows:

    Let c and d be real numbers. Define the sequence $a_1, a_2, \ldots, a_n, \ldots$ by $a_1 = c$ and for each $n \in \mathbb{N}$, $a_{n+1} = a_n + d$.

    (a) Determine formulas for a_3 through a_8.
    (b) Make a conjecture for a formula for a_n for each n for each $n \in \mathbb{N}$.
    (c) Prove that your conjecture in Exercise (10b) is correct.
11. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$, $a_2 = 5$, and that for each $n \in \mathbb{N}$, $a_{n+1} = a_n + 2a_{n-1}$. Prove that for each natural number n, $a_n = 2^n + (-1)^n$.
12. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$ and that for each $n \in \mathbb{N}$, $a_{n+1} = \sqrt{5 + a_n}$.

    (a) Calculate, or approximate, a_2 through a_6.
    (b) Prove that for each $n \in \mathbb{N}$, $a_n < 3$.
13. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$, $a_2 = 3$, and that for each $n \in \mathbb{N}$, $a_{n+2} = 3a_{n+1} - 2a_n$.

    (a) Calculate a_3 through a_6.
    (b) Make a conjecture for a formula for a_n for each n for each $n \in \mathbb{N}$.
    (c) Prove that your conjecture in Exercise (13b) is correct.
14. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$, $a_2 = 1$, and that for each $n \in \mathbb{N}$, $a_{n+2} = \dfrac{1}{2}(a_{n+1} + \dfrac{2}{a_n})$.

    (a) Calculate a_3 through a_6.
    (b) Prove that for each $n \in \mathbb{N}$, $1 \leq a_n \leq 2$.
15. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$, $a_2 = 1$, $a_3 = 1$, and for that each natural number n,

    $$a_{n+3} = a_{n+2} + a_{n+1} + a_n. \tag{4.3.7}$$

    (a) Compute a_4, a_5, a_6, and a_7.
    (b) Prove that for each natural number n with $n > 1$, $a_n \leq 2^{n-2}$.
16. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$, and for each natural number n,

    $$a_{n+1} = a_n + n \cdot n!. \tag{4.3.8}$$

    (a) Compute $n!$ for the first 10 natural numbers.
    (b) Compute a_n for the first 10 natural numbers.
    (c) Make a conjecture about a formula for a_n in terms of n that does not involve a summation or a recursion.
    (d) Prove your conjecture in Part (c).
17. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$, $a_2 = 1$, and for each $n \in \mathbb{N}$, $a_{n+2} = a_{n+1} + 3a_n$. Determine which terms in this sequence are divisible by 4 and prove that your answer is correct.
18. The Lucas numbers are a sequence of natural numbers $L_1, L_2, L_3, \ldots, L_n, \ldots$, which are defined recursively as follows:

    $bullet$ $L_1 = 1$ and $L_2 = 3$, and
    $bullet$ For each natural number n, $L_{n+2} = L_{n+1} + L_n$.

    List the first 10 Lucas numbers and the first ten Fibonacci numbers and then prove each of the following propositions. The

Second Principle of Mathematical Induction may be needed to prove some of these propositions.

(a) For each natural number n, $L_n = 2f_{n+1} - f_n$.
(b) For each $n \in \mathbb{N}$ with $n \geq 2$, $5f_n = L_{n-1} + L_{n+1}$.
(c) For each $n \in \mathbb{N}$ with $n \geq 3$, $L_n = f_{n+1} - f_{n-2}$.

19. There is a formula for the Lucas number similar to the formula for the Fibonacci numbers in Exercise (4). Let $\alpha = \dfrac{1+\sqrt{5}}{2}$ and $\beta = \dfrac{1-\sqrt{5}}{2}$. Prove that for each $n \in \mathbb{N}$, $L_n = \alpha^n + \beta^n$.
20. Use the result in Exercise (19), previously proven results from Exercise (18), or mathematical induction to prove each of the following results about Lucas numbers and Fibonacci numbers.

(a) For each $n \in \mathbb{N}$, $L_n = \dfrac{f_{2n}}{f_n}$
(b) For each $n \in \mathbb{N}$, $f_{n+1} = \dfrac{f_n + L_n}{2}$.
(c) For each $n \in \mathbb{N}$, $L_{n+1} = \dfrac{L_n + 5f_n}{2}$.
(d) For each $n \in \mathbb{N}$ with $n \geq 2$, $L_n = f_{n+1} + f_{n-1}$.

21. **Evaluation of proofs**
See the instructions for Exercise (19) on page 100 from Section 3.1.

(a)

Let f_n be the nth Fibonacci number, and let α be the positive solution of the equation $x^2 = x + 1$. So $\alpha = \dfrac{1+\sqrt{5}}{2}$. For each natural number n, $f_n \leq \alpha^{n-1}$.

Proof

We will use a proof by mathematical induction. For each natural number n, we let $P(n)$ be, "$f_n \leq \alpha^{n-1}$."

We first note that $P(1)$ is true since $f_1 = 1$ and$\alpha^0 = 1$. We also notice that $P(2)$ is true since $f_2 = 1$ and, hence, $f_2 \leq \alpha^1$.

We now let k be a natural number with $k \geq 2$ and assume that $P(1)$, $P(2)$, ..., $P(k)$ are all true. We now need to prove that $P(k+1)$ is true or that $f_{k+1} \leq \alpha^k$.

Since $P(k-1)$ and $P(k)$ are true, we know that $f_{k-1} \leq \alpha^{k-2}$ and $f_k \leq \alpha^{k-1}$. Therefore,

\[\begin{array} {rcl} {f_{k + 1}} &= & {f_k + f_{k - 1}} \ {f_{k + 1}} &\le & {\alpha ^{k - 1} + {\alpha ^{k - 2}} \ {f_{k + 1}} &\le & {\alpha ^{k - 2} (\alpha + 1).} \end{array}\]

We now use the fact that $\alpha + 1 = \alpha^2$ and the preceding inequality to obtain

$$\begin{array}{rcl} f_{k+1} & \leq & \alpha^{k-2}\alpha^2 \\ f_{k+1} & \leq & \alpha^k. \end{array} \tag{4.3.9}$$

This proves that if $P(1)$, $P(2)$, ..., $P(k)$ are true, then $P(k+1)$ is true. Hence, by the Second Principle of Mathematical Induction, we conclude that or each natural number n, $f_n \leq \alpha^{n-1}$.

Explorations and Activities

22. **Compound Interest.** Assume that R dollars is deposited in an account that has an interest rate of i for each compounding period. A compounding period is some specified time period such as a month or a year.
For each integer n with $n \leq 0$, let Vn be the amount of money in an account at the end of the nth compounding period. Then

$$\begin{array}{rcl} V_1 & = & R + i \cdot R \\ & = & R(1+i) \end{array} \qquad \begin{array}{rcl} V_2 & = & V_1 + i \cdot V_1 \\ & = & (1+i)V_1 \\ & = & (1+i)^2 R. \end{array} \tag{4.3.10}$$

(a) Explain why $V_3 = V_2 + i \cdot V_2$. Then use the formula for V2 to determine a formula for V_3 in terms of i and R.
(b) Determine a recurrence relation for V_{n+1} in terms of i and V_n.
(c) Write the recurrence relation in Part (22b) so that it is in the form of a recurrence relation for a geometric sequence. What is the initial term of the geometric sequence and what is the common ratio?
(d) Use Proposition 4.14 to determine a formula for V_n in terms of I, R, and n.

23. **The Future Value of an Ordinary Annuity.** For an **ordinary annuity**, R dollars is deposited in an account at the end of each compounding period. It is assumed that the interest rate, i, per compounding period for the account remains constant.

Let S_t represent the amount in the account at the end of the tth compounding period. S_t is frequently called the future value of the ordinary annuity.

So $S_1 = R$. To determine the amount after two months, we first note that the amount after one month will gain interest and grow to $(1+i)S_1$. In addition, a new deposit of R dollars will be made at the end of the second month. So

$$S_2 = R + (1+i)S_1 \tag{4.3.11}$$

(a) For each $n \in \mathbb{N}$, use a similar argument to determine a recurrence relation for S_{n+1} in terms of R, i, and S_n.
(b) By recognizing this as a recursion formula for a geometric series, use Proposition 4.16 to determine a formula for S_n in terms of R, i, and n that does not use a summation. Then show that this formula can be written as

$$S_n = R(\frac{(1+i)^n - 1}{i}). \tag{4.3.12}$$

(c) What is the future value of an ordinary annuity in 20 years if $200 dollars is deposited in an account at the end of each month where the interest rate for the account is 6% per year compounded monthly? What is the amount of interest that has accumulated in this account during the 20 years?

Answer

Add texts here. Do not delete this text first.

This page titled 4.3: Induction and Recursion is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

4.S: Mathematical Induction (Summary)

Important Definitions

- Inductive set, page 171
- Factorial, page 201
- Recursive definition, page 200
- Fibonacci numbers, page 202
- Geometric sequence, page 206
- Geometric series, page 206

The Various Forms of Mathematical Induction

1. **The Principle of Mathematical Induction**
   If T is a subset of $\mathbb{N}$ such that

   (a) $1 \in T$, and
   (b) For every $k \in \mathbb{N}$, if $k \in T$, then $(k+1) \in T$.

   then $T = \mathbb{N}$
   Procedure for a Proof by Mathematical Induction
   To prove $(\forall n \in \mathbb{N}$(P(n))\)

$$\begin{aligned} \text{Basis step} &: \text{Prove} P(1). \\ \text{Inductive step} &: \text{Prove that for each} k \in \mathbb{N}, \text{if} P(k) \text{is true, then} P(k+1) \text{is true.} \end{aligned} \tag{4.S.1}$$

2. **The Extended Principle of Mathematical Induction**
   Let M be an integer. If T is a subset of $\mathbb{Z}$ such that

   (a) $M \in T$, and
   (b) For every $k \in \mathbb{Z}$ with $k \geq M$, if $k \in T$, then $(k+1) \in T$.

   then T contains all integers greater than or equal to M.
   Using the Extended Principle of Mathematical Induction
   Let M be an intteger. To prove $(\forall n \in \mathbb{Z} \text{with} n \geq M)(P(n))$

$$\begin{aligned} \text{Basis step} &: \text{Prove} P(M). \\ \text{Inductive step} &: \text{Prove that for each} k \in \mathbb{Z} \text{with} k \geq M, \text{if} P(k) \text{is true, then} P(k+1) \text{is true.} \end{aligned} \tag{4.S.2}$$

   We can then conclude that $P(n)$ is true for all $n \in \mathbb{Z}$ with $n \geq M$.

3. The Second Principle of Mathematical Induction
   Let M be an integer. If T is a subset of $\mathbb{Z}$ such that

   (a) $M \in T$, and
   (b) For every $k \in \mathbb{Z}$ with $k \geq M$, if $\{M, M+1, \ldots, k\} \subseteq T$, then $(k+1) \in T$.

   then T contains all integers greater than or equal to M.
   Using the Second Principle of Mathematical Induction
   Let M be an intteger. To prove $(\forall n \in \mathbb{Z} \text{with} n \geq M)(P(n))$

$$\begin{aligned} \text{Basis step} &: \text{Prove} P(M). \\ \text{Inductive step} &: \text{Let} k \in \mathbb{Z} \text{with} k \geq M. \text{Prove that if} P(M), P(M+1), \ldots, \\ & \quad P(k) \text{are true, then} P(k+1) \text{is true.} \end{aligned} \tag{4.S.3}$$

   We can then conclude that $P(n)$ is true for all $n \in \mathbb{Z}$ with $n \geq M$.

Important Results

- **Theorem 4.9.** *Each natural number greater than 1 is either a prime number or is a product of prime numbers.*
- **Theorem 4.14**. Let $a, r \in \mathbb{R}$. If a geometric sequence is defined by $a_1 = a$ and for each $n \in \mathbb{N}$, $a_{n+1} = r \cdot a_n$, then for each $n \in \mathbb{N}$, $a_n = a \cdot r^{n-1}$.
- **Theorem 4.15.** Let $a, r \in \mathbb{R}$. If the sequence $S_1, S_2, ..., S_n, ...$ is defined by $S_1 = a$ and for each $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$, then for each $n \in \mathbb{N}$, $S_n = a + a \cdot r + a \cdot r^2 + \cdots + a \cdot r^{n-1}$. That is, the geometric series S_n is the sum of the first n terms of the corresponding geometric sequence.
- **Theorem 4.16.** Let $a, r \in \mathbb{R}$ and $r \neq 1$. If the sequence $S_1, S_2, ..., S_n, ...$ is defined by $S_1 = a$ and for each $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$, then for each $n \in \mathbb{N}$, $S_n = a(\dfrac{1 - r^n}{1 - r})$.

This page titled 4.S: Mathematical Induction (Summary) is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

CHAPTER OVERVIEW

5: Set Theory

5.1: Sets and Operations on Sets
5.2: Proving Set Relationships
5.3: Properties of Set Operations
5.4: Cartesian Products
5.5: Indexed Families of Sets
5.S: Set Theory (Summary)

Thumbnail: A Venn diagram illustrating the intersection of two sets. (Public Domain; Cepheus).

This page titled 5: Set Theory is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

5.1: Sets and Operations on Sets

Before beginning this section, it would be a good idea to review sets and set notation, including the *roster method* and *set builder notation*, in Section 2.3.

PREVIEW ACTIVITY $5.1.1$: Set Operations

In Section 2.1, we used logical operators (conjunction, disjunction, negation) to form new statements from existing statements. In a similar manner, there are several ways to create new sets from sets that have already been defined. In fact, we will form these new sets using the logical operators of conjunction (and), disjunction (or), and negation (not). For example, if the universal set is the set of natural numbers N and

$$A = \{1, 2, 3, 4, 5, 6\} \quad \text{and} \quad B = \{1, 3, 5, 7, 9\}, \tag{5.1.1}$$

- The set consisting of all natural numbers that are in A and are in B is the set $\{1, 3, 5\}$;
- The set consisting of all natural numbers that are in A or are in B is the set $\{1, 2, 3, 4, 5, 6, 7, 9\}$; and
- The set consisting of all natural numbers that are in A and are not in B is the set $\{2, 4, 6\}$.

These sets are examples of some of the most common set operations, which are given in the following definitions.

Definition: intersection

Let A and B be subsets of some universal set U. The *intersection* of A and B, written $A \cap B$ and read "A intersect B," is the set of all elements that are in both A and B. That is,

$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}. \tag{5.1.2}$$

The union of A and B, written $A \cup B$ and read "A union B," is the set of all elements that are in A or in B. That is,

$$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}. \tag{5.1.3}$$

Definition: complement

Let A and B be subsets of some universal set U. The set *difference* of A and B, or *relative complement* of B with respect to A, written $A - B$ and read "A minus B" or "the complement of B with respect to A," is the set of all elements in A that are not in B. That is,

$$A - B = \{x \in U \mid x \in A \text{ and } x \notin B\}. \tag{5.1.4}$$

The *complement* of the set A, written A^c and read "the complement of A," is the set of all elements of U that are not in A. That is,

$$A^c = \{x \in U \mid x \notin A\}. \tag{5.1.5}$$

For the rest of this preview activity, the universal set is $U = \{0, 1, 2, 3, ..., 10\}$, and we will use the following subsets of U:

$$A = \{0, 1, 2, 3, 9\} \quad \text{and} \quad B = \{2, 3, 4, 5, 6\}, \tag{5.1.6}$$

So in this case, $A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\} = \{2, 3\}$. Use the roster method to specify each of the following subsets of U.

1. $A \cup B$
2. A^c
3. B^c

We can now use these sets to form even more sets. For example,

$$A \cap B^c = \{0, 1, 2, 3, 9\} \cap \{0, 1, 7, 8, 9, 10\} = \{0, 1, 9\}. \tag{5.1.7}$$

Use the roster method to specify each of the following subsets of U.

4. $A \cup B^c$
5. $A^c \cap B^c$

6. $A^c \cup B^c$
7. $(A \cap B)^c$

? Preview Activity $5.1.2$: Venn Diagrams for Two Sets

In Preview Activity $5.1.1$, we worked with verbal and symbolic definitions of set operations. However, it is also helpful to have a visual representation of sets. *Venn diagrams* are used to represent sets by circles (or some other closed geometric shape) drawn inside a rectangle. The points inside the rectangle represent the universal set U, and the elements of a set are represented by the points inside the circle that represents the set. For example, Figure $5.1.1$ is a Venn diagram showing two sets.

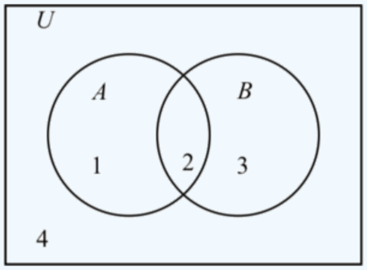


Figure $5.1.1$*: Venn Diagram for Two Sets*

In Figure $5.1.1$, the elements of A are represented by the points inside the left circle, and the elements of B are represented by the points inside the right circle. The four distinct regions in the diagram are numbered for reference purposes only. (The numbers do not represent elements in a set.) The following table describes the four regions in the diagram.

Region	Elements of U	Set
1	In A and not in B	$A - B$
2	In A and in B	$A \cap B$
3	In B and not in A	$B - A$
4	Not in A and not in B	$A^c \cap B^c$

We can use these regions to represent other sets. For example, the set $A \cup B$ is represented by regions 1, 2, and 3 or the shaded region in Figure $5.1.2$.

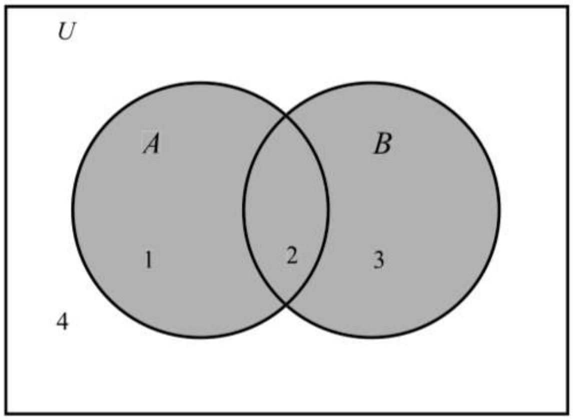


Figure $5.1.2$***:*** *Venn Diagram for* $A \cup B$

Let A and B be subsets of a universal set U. For each of the following, draw a Venn diagram for two sets and shade the region that represent the specified set. In addition, describe the set using set builder notation.

1. A^c

2. B^c
3. $A^c \cup B$
4. $A^c \cup B^c$
5. $(A \cap B)^c$
6. $(A \cup B) - (A \cap B)$

Set Equality, Subsets, and Proper Subsets

In Section 2.3, we introduced some basic definitions used in set theory, what it means to say that two sets are equal and what it means to say that one set is a subset of another set. We need one more definition.

Definition: proper subset

Let A and B be two sets contained in some universal set U. The set A is a *proper subset* of B provided that $A \subseteq B$ and $A \neq B$. When A is a proper subset of B, we write $A \subset B$.

One reason for the definition of proper subset is that each set is a subset of itself. That is,

If A is a set, then $A \subseteq A$

However, sometimes we need to indicate that a set X is a subset of Y but $X \neq Y$. For example, if

$X = \{1, 2\}$ and $Y = \{0, 1, 2, 3\}$.

then $X \subset Y$. We know that $X \subseteq Y$ since each element of X is an element of Y, but $X \neq Y$ since $0 \in Y$ and $0 \notin X$. (Also, $3 \in Y$ and $3 \notin X$.) Notice that the notations $A \subset B$ and $A \subseteq B$ are used in a manner similar to inequality notation for numbers ($a < b$ and $a \leq b$).

It is often very important to be able to describe precisely what it means to say that one set is not a subset of the other. In the preceding example, Y is not a subset of X since there exists an element of Y (namely, 0) that is not in X.

In general, the subset relation is described with the use of a universal quantifier since $A \subseteq B$ means that for each element x of U, if $x \in A$, then $x \in B$. So when we negate this, we use an existential quantifier as follows:

$$\begin{array}{lll} A \subseteq B & \text{means} & (\forall x \in U)[(x \in A) \to (x \in B)]. \\ A \nsubseteq B & \text{means} & \urcorner(\forall x \in U)[(x \in A) \to (x \in B)] \\ & & (\exists x \in U)\urcorner[(x \in A) \to (x \in B)] \\ & & (\exists x \in U)[(x \in A) \wedge (x \notin B)]. \end{array} \tag{5.1.8}$$

So we see that $A \nsubseteq B$ means that there exists an x in U such that $x \in A$ and $x \notin B$.

Notice that if $A = \emptyset$, then the conditional statement, “For each $x \in U$, if $x \in \emptyset$, then $x \in B$” must be true since the hypothesis will always be false. Another way to look at this is to consider the following statement:

$\emptyset \nsubseteq B$ means that there exists an $x \in \emptyset$ such that $x \notin B$.

However, this statement must be false since there does not exist an x in $\emptyset$. Since this is false, we must conclude that $\emptyset \subseteq B$. Although the facts that $\emptyset \subseteq B$ and $B \subseteq B$ may not seem very important, we will use these facts later, and hence we summarize them in Theorem 5.1.

Theorem 5.1

For any set B, $\emptyset \subseteq B$ and $B \subseteq B$.

In Section 2.3, we also defined two sets to be equal when they have precisely the same elements. For example,

$$\{x \in \mathbb{R} \mid x^{=}4\} = \{-2, 2\}.$$

If the two sets A and B are equal, then it must be true that every element of A is an element of B, that is, $A \subseteq B$, and it must be true that every element of B is an element of A, this is, $B \subseteq A$. Conversely, if $A \subseteq B$ and $B \subseteq A$, then A and B must have precisely the same elements. This gives us the following test for set equality:

Theorem 5.2

Let A and B be subsets of some universal set U. Then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

Progress Check 5.3: Using Set Notation

Let the universal set be $U = \{1, 2, 3, 4, 5, 6\}$, and let

$$A = \{1, 2, 4\},\ B = \{1, 2, 3, 5\},\ C = \{x \in U \mid x^2 \leq 2\}.$$

In each of the following, fill in the blank with one or more of the symbols $\subset$, $\subseteq$, =, $\neq$, $\in$ or $\notin$ so that the resulting statement is true. For each blank, include all symbols that result in a true statement. If none of these symbols makes a true statement, write nothing in the blank.

'_' allowed only in math mode

Answer

Add texts here. Do not delete this text first.

More about Venn Diagrams

In Preview Activity $5.1.2$, we learned how to use Venn diagrams as a visual representation for sets, set operations, and set relationships. In that preview activity, we restricted ourselves to using two sets. We can, of course, include more than two sets in a Venn diagram. Figure $5.1.3$ shows a general Venn diagram for three sets (including a shaded region that corresponds to $A \cap C$).

In this diagram, there are eight distinct regions, and each region has a unique reference number. For example, the set A is represented by the combination of regions 1, 2, 4, and 5, whereas the set C is represented by the combination of regions 4, 5, 6, and 7. This means that the set $A \cap C$ is represented by the combination of regions 4 and 5. This is shown as the shaded region in Figure $5.1.3$.

Finally, Venn diagrams can also be used to illustrate special relationships be- tween sets. For example, if $A \subseteq B$, then the circle representing A should be completely contained in the circle for B. So if $A \subseteq B$, and we know nothing about

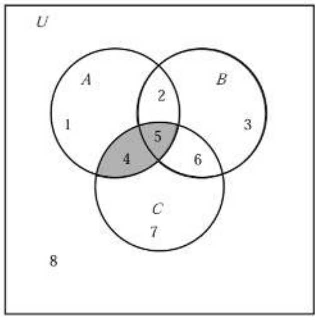


Figure 5.3: Venn Diagram for $A \cap C$

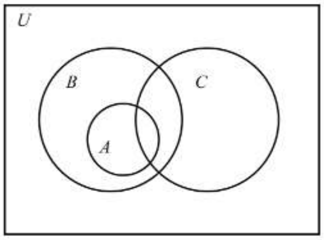


Figure 5.4: Venn Diagram Showing $A \subseteq B$

any relationship between the set C and the sets A and B, we could use the Venn diagram shown in Figure $5.1.4$.

Progress Check 5.4: Using Venn Diagrams

Let A, B, and C be subsets of a universal set U.

1. For each of the following, draw a Venn diagram for three sets and shade the region(s) that represent the specified set.

    (a) $(A \cap B) \cap C$
    (b) $(A \cap B) \cup C$
    (c) $(A^c \cup B)$
    (d) $A^c \cap (B \cup C)$
2. Draw the most general Venn diagram showing $B \subseteq (A \cup C)$.
3. Draw the most general Venn diagram showing $A \subseteq (B^c \cup C)$.

Answer

Add texts here. Do not delete this text first.

The Power Set of a Set

The symbol 2 is used to describe a relationship between an element of the universal set and a subset of the universal set, and the symbol $\subseteq$ is used to describe a relationship between two subsets of the universal set. For example, the number 5 is an integer, and so it is appropriate to write $5 \in \mathbb{Z}$. It is not appropriate, however, to write $5 \subseteq \mathbb{Z}$ since 5 is not a set. It is important to distinguish between 5 and {5}. The difference is that 5 is an integer and {5} is a set consisting of one element. Consequently, it is appropriate to write $\{5\} \subseteq \mathbb{Z}$, but it is not appropriate to write $\{5\} \in \mathbb{Z}$. The distinction between these two symbols (5 and {5}) is important when we discuss what is called the power set of a given set.

Definition: power set

If A is a subset of a universal set U, then the set whose members are all the subsets of A is called the *power set* of A. We denote the power set of A by $\mathcal{P}(A)$. Symbolically, we write

$$\mathcal{P}(A) = \{X \subseteq U \mid X \subseteq A\}.$$

That is, $X \in \mathcal{P}(A)$ if and only if $X \subseteq A$.

When dealing with the power set of A, we must always remember that $\emptyset \subseteq A$ and $A \subseteq A$. For example, if $A = \{a, b\}$, then the subsets of A are

$$\emptyset, \{a\}, \{b\}, \{a, b\}. \tag{5.1.9}$$

We can write this as

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

Now let $B = \{a, b, c\}$. Notice that $B = A \cup \{c\}$. We can determine the subsets of B by starting with the subsets of A in (5.1.10). We can form the other subsets of B by taking the union of each set in (5.1.10) with the set $\{c\}$. This gives us the following subsets of B.

$$\{c\}, \{a, c\}, \{b, c\}, \{a, b, c\}. \tag{5.1.10}$$

So the subsets of B are those sets in (5.1.10) combined with those sets in (5.1.11). That is, the subsets of B are

$$\emptyset, \{a\}, \{b\}, \{a, b\}, \{c\}, \{a, c\}, \{b, c\}, \{a, b, c\}, \tag{5.1.11}$$

which means that

$$\mathcal{P}(B) = \{\emptyset, \{a\}, \{b\}, \{a, b\}, \{c\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Notice that we could write

$$\{a, c\} \subseteq B \text{ or that } \{a, c\} \in \mathcal{P}(B).$$

Also, notice that A has two elements and A has four subsets, and B has three elements and B has eight subsets. Now, let n be a nonnegative integer. The following result can be proved using mathematical induction. (See Exercise 17).)

Theorem 5.5.

Let n be a nonnegative integer and let T be a subset of some universal set. If the set T has n elements, then the set T has 2^n subsets. That is, $\mathcal{P}(T)$ has 2^n elements.

The Cardinality of a Finite Set

In our discussion of the power set, we were concerned with the number of elements in a set. In fact, the number of elements in a finite set is a distinguishing characteristic of the set, so we give it the following name.

Definition: cardinality

The number of elements in a finite set A is called the *cardinality* of A and is denoted by card(A)

Example

card($\emptyset$) = 0;

card({a, b}) = 2

card($\mathcal{P}(\{a, b\})$) = 4

Theoretical Note: There is a mathematical way to distinguish between finite and infinite sets, and there is a way to define the cardinality of an infinite set. We will not concern ourselves with this at this time. More about the cardinality of finite and infinite sets is discussed in Chapter 9.

Standard Number Systems

We can use set notation to specify and help describe our standard number systems. The starting point is the set of **natural numbers**, for which we use the roster method.

$$\mathbb{N} = \{1, 2, 3, 4, ...\}$$

The **integers** consist of the natural numbers, the negatives of the natural numbers, and zero. If we let $\mathbb{N}^- = \{..., -4, -3, -2, -1\}$, then we can use set union and write

$$\mathbb{Z} = \mathbb{N}^- \cup \{0\} \cup \mathbb{N}.$$

So we see that $\mathbb{N} \subseteq \mathbb{Z}$, and in fact, $\mathbb{N} \subset \mathbb{Z}$.

We need to use set builder notation for the set $\mathbb{Q}$ of all **rational numbers**, which consists of quotients of integers.

$$\mathbb{Q} = \left\{\frac{m}{n} \mid m, n \in \mathbb{Z}\text{and } n \neq 0\right\}$$

Since any integer n can be written as $n = \dfrac{n}{1}$, we see that $\mathbb{Z} \subseteq \mathbb{Q}$.

We do not yet have the tools to give a complete description of the real numbers. We will simply say that the **real numbers** consist of the rational numbers and the **irrational numbers**. In effect, the irrational numbers are the complement of the set of rational numbers $\mathbb{Q}$ in $\mathbb{R}$. So we can use the notation $\mathbb{Q}^c = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$ and write

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{Q}^c \text{ and } \mathbb{Q} \cap \mathbb{Q}^c = \emptyset.$$

A number system that we have not yet discussed is the set of **complex numbers**. The complex numbers, $\mathbb{C}$, consist of all numbers of the form $a + bi$, where $a, b \in \mathbb{R}$ and $i = \sqrt{-1}$ (or $i^2 = -1$). That is,

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\text{and } i = sqrt{-1}\}.$$

We can add and multiply complex numbers as follows: If $a, b, c, d \in \mathbb{R}$, then

$$\begin{aligned} (a+bi)+(c+di) &= (a+c)+(b+d)i, \text{ and} \\ (a+bi)(c+di) &= ac+adi+bci+bdi^2 \end{aligned} \tag{5.1.12}$$

$$= \quad (ac - bd) + (ad + bc)i.$$

Exercises for Section 5.1

1. Assume the universal set is the set of real numbers. Let

   $A = \{-3, -2, 2, 3\}.$
   $B = \{x \in \mathbb{R} \mid x^2 = 4 \text{ or } x^2 = 9\},$
   $C = \{x \in \mathbb{R} \mid x^2 + 2 = 0\},$
   $D = \{x \in \mathbb{R} \mid x > 0\}.$

   Respond to each of the following questions. In each case, explain your answer.

   (a) Is the set A equal to the set B?
   (b) Is the set A a subset of the set B?
   (c) Is the set C equal to the set D?
   (d) Is the set C a subset of the set D?
   (e) Is the set A a subset of the set D?
2. (a) Explain why the set $\{a, b\}$ is equal to the set $\{b, a\}$.
   (b) Explain why the set $\{a, b, b, a, c\}$ is equal to the set $\{b, c, a\}$.
3. Assume that the universal set is the set of integers. Let

   $A = \{-3, -2, 2, 3\}.$
   $B = \{x \in \mathbb{Z} \mid x^2 \le 9\},$
   $C = \{x \in \mathbb{Z} \mid x \ge -3\},$
   $D = \{1, 2, 3, 4\},$

   In each of the following, fill in the blank with one or more of the symbols $\subset$, $\subseteq$, $\not\subseteq$, $=$, $\neq$, $\in$ or $\notin$ so that the resulting statement is true. For each blank, include all symbols that result in a true statement. If none of these symbols makes a true statement, write nothing in the blank.

   '_' allowed only in math mode

4. Write all of the proper subset relations that are possible using the sets of numbers $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$.
5. For each statement, write a brief, clear explanation of why the statement is true or why it is false.

   (a) The set $\{a, b\}$ is a subset of $\{a, c, d, e\}$.
   (b) The set $\{-2, 0, 2\}$ is equal to $\{x \in \mathbb{Z} \mid x \text{ is even and } x^2 < 5\}$.
   (c) The empty set $\emptyset$ is a subset of $\{1\}$.
   (d) If $A = \{a, b\}$, then the set $\{a\}$ is a subset of $\mathcal{P}(A)$.
6. Use the definitions of set intersection, set union, and set difference to write useful negations of these definitions. That is, complete each of the following sentences

   (a) $x \notin A \cap B$ if and only if ... .
   (b) $x \notin A \cup B$ if and only if ... .
   (c) $x \notin A - B$ if and only if ... .
7. Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, and let

   $A = \{3, 4, 5, 6, 7\}$
   $B = \{1, 5, 7, 9\}$
   $C = \{3, 6, 9\}$
   $D = \{2, 4, 6, 8\}$

Use the roster method to list all of the elements of each of the following sets.
(a) $A \cap B$
(b) $A \cup B$
(c) $(A \cup B)^c$
(d) $A^c \cap B^c$
(e) $(A \cup B) \cap C$
(f) $A \cap C$
(g) $B \cap C$
(h) $(A \cap C) \cup (B \cap C)$
(i) $B \cap D$
(j) $(B \cap D)^c$
(k) $A - D$
(l) $B - D$
(m) $(A - D) \cup (B - D)$
(n) $(A \cup B) - D$

8. Let $U = \mathbb{N}$, and let

$A = \{x \in \mathbb{N} \mid x \geq 7\}$,
$B = \{x \in \mathbb{N} \mid x \text{ is odd}\}$,
$C = \{x \in \mathbb{N} \mid x \text{ is a multiple of } 3\}$,
$D = \{x \in \mathbb{N} \mid x \text{ is even}\}$,

Use the roster method to list all of the elements of each of the following sets.

(a) $A \cap B$
(b) $A \cup B$
(c) $(A \cup B)^c$
(d) $A^c \cap B^c$
(e) $(A \cup B) \cap C$
(f) $(A \cap C) \cup (B \cap C)$
(g) $B \cap D$
(h) $(B \cap D)^c$
(i) $A - D$
(j) $B - D$
(k) $(A - D) \cup (B - D)$
(l) $(A \cup B) - D$

9. let P, Q, R, and S, be subsets of a universal set U, Assume that $(P - Q) \subseteq (R \cap S)$.

(a) Complete the following sentence:
For each $x \in U$, if $x \in (P - Q)$, then ... .
(b) Write a useful negation of the statement in Part (9a).
(c) Write the contrapositive of the statement in Part (9a).

10. Let U be the universal set. Consider the following statement:

For all A, B, and C that are subsets of U, if $A \subseteq B$, then $B^c \subseteq A^c$.

(a) Identify three conditional statements in the given statement.
(b) Write the contrapositive of this statement.
(c) Write the negation of this statement.

11. Let A, B, and C be subsets of some universal sets U. Draw a Venn diagram for each of the following situations.

(a) $A \subseteq C$

(b) $A \cap B = \emptyset$
(c) $A \not\subseteq B$, $B \not\subseteq A$, $C \subseteq A$, and $C \not\subseteq B$
(d) $A \subseteq B$, $C \subseteq B$, and $A \cap C = \emptyset$

12. Let A, B, and C be subsets of some universal sets U. For each of the following, draw a general Venn diagram for the three sets and then shade the indicated region.

    (a) $A \cap B$
    (b) $A \cap C$
    (c) $(A \cap B) \cup (A \cap C)$
    (d) $B \cup C$
    (e) $A \cap (B \cup C)$
    (f) $(A \cap B) - C$
13. We can extend the idea of consecutive integers (See Exercise (2) in Section 3.5) to represent four consecutive integers as m, $m+1$, $m+2$, and $m+3$, where m is an integer. There are other ways to represent four consecutive integers. For example, if $k \in \mathbb{Z}$, then $k-1$, k, $k+1$, and $k+2$ are four consecutive integers.

    (a) Prove that for each $n \in \mathbb{Z}$, n is the sum of four consecutive integers if and only if $n \equiv 2$ (mod 4).
    (b) Use set builder notation or the roster method to specify the set of integers that are the sum of four consecutive integers.
    (c) Specify the set of all natural numbers that can be written as the sum of four consecutive natural numbers.
    (d) Prove that for each $n \in \mathbb{Z}$, n is the sum of eight consecutive integers if and only if $n \equiv 4$ (mod 8).
    (e) Use set builder notation or the roster method to specify the set of integers that are the sum of eight consecutive integers.
    (f) Specify the set of all natural numbers can be written as the sum of eight consecutive natural numbers.
14. One of the properties of real numbers is the so-called **Law of Trichotomy**, which states that if $a, b \in \mathbb{R}$, then exactly one of the following is true:

- $a < b$;
- $a = b$;
- $a > b$.

Is the following proposition concerning sets true or false? Either provide a proof that it is true or a counterexample showing it is false.

If A and B are subsets of some universal set, then exactly one of the following is true:

- $A \subseteq B$;
- $A = B$;
- $B \subseteq A$.

Explorations and Activities

15. **Intervals of Real Numbers.** In previous mathematics courses, we have frequently used subsets of the real numbers called intervals. There are some common names and notations for intervals. These are given in the following table, where it is assumed that a and b are real numbers and $a < b$.

Interval Notation	Set Notation	Name
(a, b) =	$\{x \in \mathbb{R} \mid a < x < b\}$	Open interval from a to b
$[a, b]$ =	$\{x \in \mathbb{R} \mid a \le x \le b\}$	Closed interval from a to b
$[a, b)$ =	$\{x \in \mathbb{R} \mid a \le x < b\}$	Half-open interval
$(a, b]$ =	$\{x \in \mathbb{R} \mid a < x \le b\}$	Half-open interval
$(a, +\infty)$ =	$\{x \in \mathbb{R} \mid x > a\}$	Open ray
$(-\infty, b)$ =	$\{x \in \mathbb{R} \mid x < b\}$	Open ray
$[a, +\infty)$ =	$\{x \in \mathbb{R} \mid x \ge a\}$	Closed ray

$(-\infty, b] =$	$\{x \in \mathbb{R} \mid x \le b\}$	Closed ray

(a) Is (a, b) a proper subset of $(a, b]$? Explain.
(b) Is $[a, b]$ a subset of $(a, +\infty)$? Explain.
(c) Use interval notation to describe

i. the intersection of the interval $[-3, 7]$ with the interval $(5, 9]$;
ii. the union of the interval $[-3, 7]$ with the interval $(5, 9]$;
iii. the set difference $[-3, 7] - (5, 9]$.

(d) Write the set $\{x \in \mathbb{R} \mid |x| \le 0.01\}$ using interval notation.
(e) Write the set $\{x \in \mathbb{R} \mid |x| > 2\}$ as the union of two intervals.

16. **More Work with Intervals**. For this exercise, use the interval notation described in Exercise 15.

(a) Determine the intersection and union of $[2, 5]$ and $[-1, +\infty)$.
(b) Determine the intersection and union of $[2, 5]$ and $[3.4, +\infty)$.
(c) Determine the intersection and union of $[2, 5]$ and $[7, +\infty)$.

Now let a, b and c be real numbers with $a < b$.

(d) Explain why the intersection of $[a, b]$ and $[c, +\infty)$ is either a closed interval, a set with one element, or the empty set.
(e)Explain why the union of $[a, b]$ and $[c, +\infty)$ is either a closed ray or the union of a closed interval and a closed ray.

17. **Proof of Theorem 5.5.** To help with the proof by induction of Theorem 5.5, we first prove the following lemma. (The idea for the proof of this lemma was illustrated with the discussion of power set after the definition on page 222.)

Lemma 5.6

Let A and B be subsets of some universal set. If $A = B \cup \{x\}$, where $x \notin B$, then any subset of A is either a subset of B or a set of the form $C \cup \{x\}$, where C is a subset of B.

Proof

Let A and B be subsets of some universal set, and assume that $A = B \cup \{x\}$ where $x \notin B$. Let Y be a subset of A. We need to show that Y is a subset of B or that $Y = C \cup \{x\}$, where C is some subset of B. There are two cases to consider: (1) x is not an element of Y, and (2) x is an element of Y.

Case 1: Assume that $x \notin Y$. Let $y \in Y$. Then. $y \in A$ and $y \ne x$. Since

$$A = B \cup \{x\},$$

this means that y must be in B. Therefore, $Y \subseteq B$.

Case 2: Assume that $x \in Y$. In this case, let $C = Y - \{x\}$. Then every element of C is an element of B. Hence, we can conclude that $C \subseteq B$ and that $Y = C \cup \{x\}$.

Cases (1) and (2) show that if $Y \subseteq A$, then $Y \subseteq B$ or $Y = C \cup \{x\}$, where $C \subseteq B$.

To begin the induction proof of Theorem 5.5, for each nonnegative integer n, we let $P(n)$ be, “If a finite set has exactly n elements, then that set has exactly 2^n subsets.”

(a) Verify that $P(0)$ is true. (This is the basis step for the induction proof.)
(b) Verify that $P(1)$ and $P(2)$ are true.
(c) Now assume that k is a nonnegative integer and assume that $P(k)$ is true. That is, assume that if a set has k elements, then that set has 2^k subsets. (This is the inductive assumption for the induction proof.) Let T be a subset of the universal set with $\text{card}(T) = k + 1$, and let $x \in T$. Then the set $B = T - \{x\}$ has k elements.

Now use the inductive assumption to determine how many subsets B has. Then use Lemma 5.6 to prove that T has twice as many subsets as B. This should help complete the inductive step for the induction proof.

Answer

Add texts here. Do not delete this text first.

This page titled 5.1: Sets and Operations on Sets is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

5.2: Proving Set Relationships

Preview Activity $5.2.1$: Working with Two Specific Sets

Let S be the set of all integers that are multiples of 6, and let T be the set of all even integers.

1. List at least four different positive elements of S and at least four different negative elements of S. Are all of these integers even?
2. Use the roster method to specify the sets S and T. (See Section 2.3 for a review of the roster method.) Does there appear to be any relationship between these two sets? That is, does it appear that the sets are equal or that one set is a subset of the other set?
3. Use set builder notation to specify the sets S and T. (See Section 2.3 for a review of the set builder notation.)
4. Using appropriate definitions, describe what it means to say that an integer x is a multiple of 6 and what it means to say that an integer y is even.
5. In order to prove that S is a subset of T, we need to prove that for each integer x, if $x \in S$, then $x \in T$.

   Complete the know-show table in Table 5.1 for the proposition that S is a subset of T.

   This table is in the form of a proof method called the **choose-an-element method**. This method is frequently used when we encounter a universal quantifier in a statement in the backward process. (In this case, this is Step $Q1$.) The key is that we have to prove something about all elements in $\mathbb{Z}$. We can then add something to the forward process by choosing an arbitrary element from the set S. (This is done in Step $P1$.) This does not mean that we can choose a specific element of S. Rather, we must give the arbitrary element a name and use only the properties it has by being a member of the set S. In this case, the element is a multiple of 6.

Table 5.1: Know-show table for Preview Activity $5.2.1$

Step	Know	Reason
P	S is the set of all integers that are multiples of 6. T is the set of all even. integers.	Hypothesis
$P1$	Let $x \in S$.	Choose an arbitrary element of S.
$P2$	$(\exists m \in \mathbb{Z})(x = 6m)$	Definition of "multiple"
...	...	...
$Q2$	x is an element T.	x is even
$Q1$	$(\forall x \in \mathbb{Z})[(x \in S) \to (x \in T)]$	Step $P1$ and Step $Q2$
Q	$S \subseteq T$.	Definition of "subset"
Step	**Show**	**Reason**

Preview Activity $5.2.2$: Working with Venn Diagrams

1. Draw a Venn diagram for two sets, A and B, with the assumption that A is a subset of B. On this Venn diagram, lightly shade the area corresponding to A^c. Then, determine the region on the Venn diagram that corresponds to B^c. What appears to be the relationship between A^c and B^c? Explain.
2. Draw a general Venn diagram for two sets, A and B. First determine the region that corresponds to the set $A - B$ and then, on the Venn diagram, shade the region corresponding to $A - (A - B)$ and shade the region corresponding to $A \cap B$. What appears to be the relationship between these two sets? Explain.

In this section, we will learn how to prove certain relationships about sets. Two of the most basic types of relationships between sets are the equality relation and the subset relation. So if we are asked a question of the form, “How are the sets A and B related?”, we can answer the question if we can prove that the two sets are equal or that one set is a subset of the other set. There are other ways to answer this, but we will concentrate on these two for now. This is similar to asking a question about how two real numbers are related. Two real numbers can be related by the fact that they are equal or by the fact that one number is less than the other number.

The Choose-an-Element Method

The method of proof we will use in this section can be called the **choose-an-element method**. This method was introduced in Preview Activity $5.2.1$. This method is frequently used when we encounter a universal quantifier in a statement in the backward process. This statement often has the form

For each element with a given property, something happens.

Since most statements with a universal quantifier can be expressed in the form of a conditional statement, this statement could have the following equivalent form:

If an element has a given property, then something happens.

We will illustrate this with the proposition from Preview Activity $5.2.1$. This proposition can be stated as follows:

> *Let S be the set of all integers that are multiples of 6, and let T be the set of all even integers. Then S is a subset of T.*

In Preview Activity $5.2.1$, we worked on a know-show table for this proposition. The key was that in the backward process, we encountered the following statement:

> Each element of S is an element of T or, more precisely, if $x \in S$, then $x \in T$.

In this case, the “element” is an integer, the “given property” is that it is an element of S, and the “something that happens” is that the element is also an element of T. One way to approach this is to create a list of all elements with the given property and verify that for each one, the “something happens.” When the list is short, this may be a reasonable approach. However, as in this case, when the list is infinite (or even just plain long), this approach is not practical.

We overcome this difficulty by using the **choose-an-element method**, where we choose an arbitrary element with the given property. So in this case, we choose an integer x that is a multiple of 6. We cannot use a specific multiple of 6 (such as 12 or 24), but rather the only thing we can assume is that the integer satisfies the property that it is a multiple of 6. This is the key part of this method.

> *Whenever we choose an arbitrary element with a given property, we are not selecting a specific element. Rather, the only thing we can assume about the element is the given property.*

It is important to realize that once we have chosen the arbitrary element, we have added information to the forward process. So in the know-show table for this proposition, we added the statement, “Let $x \in S$” to the forward process. Following is a completed proof of this proposition following the outline of the know-show table from Preview Activity $5.2.1$.

Proposition 5.7

Let S be the set of all integers that are multiples of 6, and let T be the set of all even integers. Then S is a subset of T.

Proof

Let S be the set of all integers that are multiples of 6, and let T be the set of all even integers. We will show that S is a subset of T by showing that if an integer x is an element of S, then it is also an element of T.

Let $x \in S$. (**Note**: The use of the word “let” is often an indication that the we are choosing an arbitrary element.) This means that x is a multiple of 6. Therefore, there exists an integer m such that

$$x = 6m.$$

Since $6 = 2 \cdot 3$, this equation can be written in the form

$$x = 2(3m).$$

By closure properties of the integers, 3m is an integer. Hence, this last equation proves that x must be even. Therefore, we have shown that if x is an element of S, then x is an element of T, and hence that $S \subseteq T$.

Having proved that S is a subset of T, we can now ask if S is actually equal to T. The work we did in Preview Activity $5.2.1$ can help us answer this question. In that preview activity, we should have found several elements that are in T but not in S. For example, the integer 2 is in T since 2 is even but $2 \notin S$ since 2 is not a multiple of 6. Therefore, $S \neq T$ and we can also conclude that S is a proper subset of T.

One reason we do this in a "two-step" process is that it is much easier to work with the subset relation than the proper subset relation. The subset relation is de- fined by a conditional statement and most of our work in mathematics deals with proving conditional statements. In addition, the proper subset relation is a conjunction of two statements ($S \subseteq T$ and $S \neq T$) and so it is natural to deal with the two parts of the conjunction separately.

Progress Check 5.8: Subsets and Set Equality

Let $A = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 9\}$ and let $B = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 3\}$

1. Is the set A a subset of B? Justify your conclusion.
2. Is the set A equal to the set B? Justify your conclusion.

Answer

Add texts here. Do not delete this text first.

Progress Check 5.9: Using the Choose-an-Element Method

The Venn diagram in Preview Activity $5.2.2$ suggests that the following proposition is true.

Proposition 5.10.

Let A and B be subsets of the universal set U. If $A \subseteq B$, then $B^c \subseteq A^c$.

1. The conclusion of the conditional statement is $B^c \subseteq A^c$. Explain why we should try the choose-an-element method to prove this proposition.
2. Complete the following know-show table for this proposition and explain exactly where the choose-an-element method is used.

Step	**Know**	**Reason**
P	$A \subseteq B$	Hypothesis
$P1$	Let $x \in B^c$.	Choose an arbitrary element of B^c.
$P2$	If $x \in A$, then $x \in B$.	Definition of "subset"
...	...	...
$Q1$	If $x \in B^c$, then $x \in A^c$.	
Q	$B^c \subseteq A^c$	Definition of "subset"
Step	**Show**	**Reason**

Answer

Add texts here. Do not delete this text first.

Proving Set Equality

One way to prove that two sets are equal is to use Theorem 5.2 and prove each of the two sets is a subset of the other set. In particular, let A and B be subsets of some universal set. Theorem 5.2 states that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

In Preview Activity $5.2.2$, we created a Venn diagram that indicated that $A-(A-B)=A\cap B$. Following is a proof of this result. Notice where the choose-an-element method is used in each case.

Proposition 5.11.

Let A and B be subsets of some universal set. Then $A-(A-B)=A\cap B$.

Proof

Let A and B be subsets of some universal set. We will prove that $A-(A-B)=A\cap B$ by proving that $A-(A-B)\subseteq A\cap B$ and that $A\cap B\subseteq A-(A-B)$.

First, let $x\in A-(A-B)$. This means that

$$x\in A \text{ and } x\notin (A-B).$$

We know that an element is in $(A-B)$ if and only if it is in A and not in B. Since $x\notin (A-B)$, we conclude that $x\notin A$ or $x\in B$. However, we also know that $x\in A$ and so we conclude that $x\in B$. This proves that

$$x\in A \text{ and } x\in B.$$

This means that $x\in A\cap B$, and hence we have proved that $A-(A-B)\subseteq A\cap B$.

Now we choose $y\in A\cap B$. This means that

$$y\in A \text{ and } y\in B.$$

We note that $y\in (A-B)$ if and only if $y\in A$ and $y\notin B$ and hence, $y\notin (A-B)$ if and only if $y\notin A$ or $y\in B$. Since we have proved that $y\in B$, we conclude that $y\notin (A-B)$, and hence, we have established that $y\in A$ and $y\notin (A-B)$. This proves that if $y\in A\cap B$, then $y\in A-(A-B)$ and hence, $A\cap B\subseteq A-(A-B)$.

Since we have proved that $A-(A-B)\subseteq A\cap B$ and $A\cap B\subseteq A-(A-B)$ we conclude that $A-(A-B)=A\cap B$.

Progress Check 5.12: Set Equality

Prove the following proposition. To do so, prove each set is a subset of the other set by using the choose-an-element method.

Proposition 5.13.

Let A and B be subsets of some universal set. Then $A-B=A\cap B^c$.

Answer

Add texts here. Do not delete this text first.

Disjoint Sets

Earlier in this section, we discussed the concept of set equality and the relation of one set being a subset of another set. There are other possible relationships between two sets; one is that the sets are disjoint. Basically, two sets are disjoint if and only if they have nothing in common. We express this formally in the following definition.

Definition: disjoint

Let A and B be subsets of the universal set U. The sets A and B are said to be *disjoint* provided that $A\cap B=\emptyset$.

For example, the Venn diagram in Figure 5.5 shows two sets A and B with $A\subseteq B$. The shaded region is the region that represents B^c. From the Venn diagram, it appears that $A\cap B^c=\emptyset$. This means that A and B^c are disjoint. The preceding example suggests that the following proposition is true:

$$\text{If } A\subseteq B, \text{ then } A\cap B^c=\emptyset.$$

If we would like to prove this proposition, a reasonable “backward question” is, “How do we prove that a set (namely $A \cap B^c$) is equal to the empty set?”

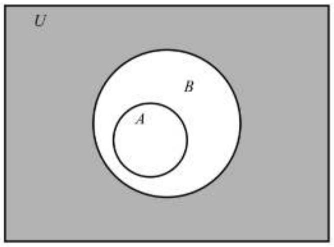


Figure 5.5: Venn Diagram with $A \subseteq B$

This question seems difficult to answer since how do we prove that a set is empty? This is an instance where proving the contrapositive or using a proof by contradiction could be reasonable approaches. To illustrate these methods, let us assume the proposition we are trying to prove is of the following form:

If P, then $T = \emptyset$.

If we choose to prove the contrapositive or use a proof by contradiction, we will assume that $T \neq \emptyset$. These methods can be outlined as follows:

- The contrapositive of “If P, then $T = \emptyset$” is, “If $T \neq \emptyset$, then $\urcorner P$.” So in this case, we would assume $T \neq \emptyset$ and try to prove $\urcorner P$.
- Using a proof by contradiction, we would assume P and assume that $T \neq \emptyset$. From these two assumptions, we would attempt to derive a contradiction.

One advantage of these methods is that when we assume that $T \neq \emptyset$, then we know that there exists an element in the set T. We can then use that element in the rest of the proof. We will prove one of th the conditional statements for Proposition 5.14 by proving its contrapositive. The proof of the other conditional statement associated with Proposition 5.14 is Exercise (10).

Proposition 5.14

Let A and B be subsets of some universal set. Then $A \subseteq B$ if and only if $A \cap B^c = \emptyset$.

Proof

Let A and B be subsets of some universal set. We will first prove that if $A \subseteq B$, then $A \cap B^c = \emptyset$, by proving its contrapositive. That is, we will prove

If $A \cap B^c \neq \emptyset$, then $A \not\subseteq B$.

So assume that $A \cap B^c \neq \emptyset$. We will prove that $A \not\subseteq B$ by proving that there must exist an element x such that $x \in A$ and $x \notin B$.

Since $A \cap B^c \neq \emptyset$, there exists an element x that is in $A \cap B^c$. This means that

$x \in A$ and $x \in B^c$.

Now the fact that $x \in B^c$ means that $x \notin B$. Hence, we can conclude that

$x \in A$ and $x \notin B$.

This means that $A \not\subseteq B$, and hence, we have proved that if $A \cap B^c \neq \emptyset$, then $A \not\subseteq B$, and therefore, we have proved that if $A \subseteq B$, then $A \cap B^c = \emptyset$.

The proof that if $A \cap B^c = \emptyset$, then $A \subseteq B$ is Exercise (10).

? Progress Check 5.15: Proving Two Sets Are Disjoint

It has been noted that it is often possible to prove that two sets are disjoint by using a proof by contradiction. In this case, we assume that the two sets are not disjoint and hence, there intersection is not empty. Use this method to prove that the following two sets are disjoint.

$A = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod{12}\}$ and $B = \{y \in \mathbb{Z} \mid y \equiv 2 \pmod{8}\}$

Answer

Add texts here. Do not delete this text first.

A Final Comment

We have used the choose-an-element method to prove Propositions 5.7, 5.11, and 5.14. Proofs involving sets that use this method are sometimes referred to **aselement-chasing proofs**. This name is used since the basic method is to choose an arbitrary element from one set and "chase it" until you prove it must be in another set.

? Exercises for Section 5.2

1. Let $A = \{x \in \mathbb{R} \mid x^2 < 4\}$ and let $B = \{x \in \mathbb{R} \mid x < 2\}$

   (a) Is $A \subseteq B$? Justify your conclusion with a proof or a counterexample.
   (b) Is $B \subseteq A$? Justify your conclusion with a proof or a counterexample.
2. Let A, B, and C be subsets of a universal set U.

   (a) Draw a Venn diagram with $A \subseteq B$ and $B \subseteq C$. Does it appear that $A \subseteq C$?
   (b) Prove the following proposition:
   If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
   Note: This may seem like an obvious result. However, one of the reasons for this exercise is to provide practice at properly writing a proof that one set is a subset of another set. So we should start the proof by assuming that $A \subseteq B$ and $B \subseteq C$. Then we should choose an arbitrary element of A.
3. Let $A = \{x \in \mathbb{Z} \mid x \equiv 7 \pmod{8}\}$ and $B = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod{4}\}$.

   (a) List at least five different elements of the set A and at least five elements of the set B.
   (b) Is $A \subseteq B$? Justify your conclusion with a proof or a counterexample.
   (c) Is $B \subseteq A$? Justify your conclusion with a proof or a counterexample.
4. Let $C = \{x \in \mathbb{Z} \mid x \equiv 7 \pmod{9}\}$ and $D = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{3}\}$.

   (a) List at least five different elements of the set C and at least five elements of the set D.
   (b) Is $C \subseteq D$? Justify your conclusion with a proof or a counterexample.
   (c) Is $D \subseteq C$? Justify your conclusion with a proof or a counterexample.
5. In each case, determine if $A \subseteq B$, $B \subseteq A$, $A = B$, or $A \cap B = \emptyset$ or none of these.

   (a) $A = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod{3}\}$ and $B = \{y \in \mathbb{Z} \mid 6 \text{ divides } (2y - 4)\}$.
   (b) $A = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod{4}\}$ and $B = \{y \in \mathbb{Z} \mid 3 \text{ divides } (y - 2)\}$.
   (c) $A = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{5}\}$ and $B = \{x \in \mathbb{Z} \mid y \equiv 7 \pmod{10}\}$
6. To prove the following set equalities, it may be necessary to use some of the properties of positive and negative real numbers. For example, it may be necessary to use the facts that:

   - The product of two real numbers is positive if and only if the two real numbers are either both positive or are both negative.
   - The product of two real numbers is negative if and only if one of the two numbers is positive and the other is negative.

   For example, if $x(x-2) < 0$, then we can conclude that either (1) $x < 0$ and $x - 2 > 0$ or (2) $x > 0$ and $x - 2 < 0$. However, in the first case, we must have $x < 0$ and $x > 2$, and this is impossible. Therefore, we conclude that $x > 0$ and $x - 2 < 0$, which means that $0 < x < 2$.

Use the choose-an-element method to prove each of the following:

(a) $\{x \in \mathbb{R} \mid x^2 - 3x - 10 < 0\} = \{x \in \mathbb{R} \mid \ -2 < x < 5\}$
(b) $\{x \in \mathbb{R} \mid x^2 - 5x + 6 < 0\} = \{x \in \mathbb{R} \mid 2 < x < 3\}$
(c) $\{x \in \mathbb{R} \mid x^2 \geq 4\} = \{x \in \mathbb{R} \mid x \leq -2\} \, cup \{x \in \mathbb{R} \mid x \geq 2\}$

7. Let A and B be subsets of some universal set U. Prove each of the following:

   (a) $A \cap B \subseteq A$
   (b) $A \subseteq A \cup B$
   (c) $A \cap A = A$
   (d) $A \cup A = A$
   (e) $A \cap \emptyset = \emptyset$
   (f) $A \cup \emptyset = A$

8. Let A and B be subsets of some universal set U. From Proposition 5.10, we know that if $A \subseteq B$, then $B^c \subseteq A^c$. Now prove the following proposition:

   For all sets (A\) and B be subsets of some universal set U, $A \subseteq B$ if and only if $B^c \subseteq A^c$.

9. Is the following proposition true or false? Justify your conclusion with a proof or a counterexample.

   For all sets (A\) and B be subsets of some universal set U, the sets $A \cap B$ and $A - B$ are disjoint.

10. Complete the proof of Proposition 5.14 by proving the following conditional statement:

    Let (A\) and B be subsets of some universal set. If $A \cap B^c = \emptyset$, then $A \subseteq B$.

11. Let A, B, C, and D be subsets of some universal set U. Are the following propositions true or false? Justify your conclusions.

    (a) If $A \subseteq B$ and $C \subseteq D$ and A and C are disjoint, then B and D are disjoint.
    (b) If $A \subseteq B$ and $C \subseteq D$ and B and D are disjoint, then A and C are disjoint.

12. Let A, B, and C be subsets of a universal set U. Prove:

    (a) If $A \subseteq B$, then $A \cap C \subseteq B \cap C$.
    (b) If $A \subseteq B$, then $A \cup C \subseteq B \cup C$.

13. Let A, B, and C be subsets of a universal set U. Are the following propositions true or false? Justify your conclusions.

    (a) If $A \cap C \subseteq B \cap C$, then $A \subseteq B$.
    (b) If $A \cup C \subseteq B \cup C$, then $A \subseteq B$.
    (c) If $A \cup C = B \cup C$, then $A = B$.
    (d) If $A \cap C = B \cup C$, then $A = B$.
    (e) If $A \cup C = B \cup C$ and $A \cap C = B \cap C$, then $A = B$.

14. Prove the following proposition:

    For all sets A, B, and C that are subsets of some universal set, if $A \cap B = A \cap C$ and $A^c \cap B = A^c \cap C$, then $B = C$.

15. Are the following biconditional statements true or false? Justify your conclusion. If a biconditional statement is found to be false, you should clearly determine if one of the conditional statements within it is true and provide a proof of this conditional statement.

    (a) For all subsets A and B of some universal set U, $A \subseteq B$ if and only if $A \cap B^c = \emptyset$.
    (b) For all subsets A and B of some universal set U, $A \subseteq B$ if and only if $A \cup B = B$.
    (c) For all subsets A and B of some universal set U, $A \subseteq B$ if and only if $A \cap B = A$.

(d) For all subsets A, B, and C of some universal set U, $A \subseteq B \cup C$ if and only if $A \subseteq B$ or $A \subseteq C$.
(e) For all subsets A, B, and C of some universal set U, $A \subseteq B \cup C$ if and only if $A \subseteq B$ and $A \subseteq C$.

16. Let S, T, X, and Y be subsets of some universal set. Assume that

(i) $S \cup T \subseteq X \cup Y$; (ii) $S \cap T = \emptyset$; and (iii) $X \subseteq S$.

(a) Using assumption (i), what conclusion(s) can be made if it is known that $a \in T$?
(b) Using assumption (ii), what conclusion(s) can be made if it is known that $a \in T$?
(c) Using all three assumptions, either prove that $T \subseteq Y$ or explain why it is not possible to do so.

17. **Evaluation of Proofs**
See the instructions for Exercise (19) on page 100 from Section 3.1.

✎ (a)

Let A, B, and C be subsets of some universal set. If $A \not\subseteq B$ and $B \not\subseteq C$, then $A \not\subseteq C$.

Proof

We assume that A, B, and C be subsets of some universal set and that $A \not\subseteq B$ and $B \not\subseteq C$. This means that there exists an element x in A that is not in B and there exists an element x that is in B and not in C. Therefore, $x \in A$ and $x \notin C$, and we have proved that $A \not\subseteq C$.

✎ (b)

Let A, B, and C be subsets of some universal set. If $A \cap B = A \cap C$, then $B = C$.

Proof

We assume that $A \cap B = A \cap C$ and prove that $B = C$. We will first prove that $B \subseteq C$.

So let $x \in B$. If $x \in A$, then $x \in A \cap B$, and hence, $x \in A \cap C$. From this we can conclude that $x \in C$. If $x \notin A$, then $x \notin A \cap B$, and hence, $x \notin A \cap C$. However, since $x \notin A$, we may conclude that $x \in C$. Therefore, $B \subseteq C$.

The proof that $C \subseteq B$ may be done in a similar manner. Hence, $B = C$.

✎

Let A, B, and C be subsets of some universal set. If $A \not\subseteq B$ and $B \subseteq C$, then $A \not\subseteq C$.

Proof

Assume that $A \not\subseteq B$ and $B \subseteq C$. Since $A \not\subseteq B$, there exists an element x such that $x \in A$ and $x \notin B$. Since $B \subseteq C$, we may conclude that $x \notin C$. Hence, $x \in A$ and $x \notin C$, and we have proved that $A \not\subseteq C$.

Explorations and Activities

18. Using the Choose-an-Element Method in a Different Setting. We have used the choose-an-element method to prove results about sets. This method, however, is a general proof technique and can be used in settings other than set theory. It is often used whenever we encounter a universal quantifier in a statement in the backward process. Consider the following proposition.

Proposition 5.16.

Let a, b and t be integers with $t \neq 0$. If t divides a and t divides b, then for all integers x and y, t divides $(ax + by)$.

(a) Whenever we encounter a new proposition, it is a good idea to explore the proposition by looking at specific examples. For example, let $a = 20$, $b = 12$, and $t = 4$. In this case, $t \mid a$ and $t \mid b$. In each of the following cases, determine the value of $(ax + by)$

and determine if t divides $(ax + by)$.

i. $x = 1$, $y = 1$.
ii. $x = 1$, $y = -1$.
iii. $x = 2$, $y = 2$.
iv. $x = 2$, $y = -3$.
v. $x = -2$, $y = 3$.
vi. $x = -2$, $y = -5$.

(b) Repeat Part (18a) with $a = 21$, $b = 6$, and $t = 3$.

Notice that the conclusion of the conditional statement in this proposition involves the universal quantifier. So in the backward process, we would have

> Q: For all integers x and y, t divides $ax + by$.

The “elements” in this sentence are the integers x and y. In this case, these integers have no “given property” other than that they are integers. The “something that happens” is that t divides $(ax + by)$. This means that in the forward process, we can use the hypothesis of the proposition and choose integers x and y. That is, in the forward process, we could have

> P: a, b, and t are integers with $t \neq 0$, t divides a and t divides b.
>
> $P1$: Let $x \in \mathbb{Z}$ and let $y \in \mathbb{Z}$.

(c) Complete the following proof of Proposition 5.16.

Proof. Let a, b and t be integers with $t \neq 0$, and assume that t divides a and t divides b. We will prove that for all integers x and y, t dibides $(ax + by)$.

So let $x \in \mathbb{Z}$ and let $y \in \mathbb{Z}$. Since t divides a, there exists an integer m such that ... .

Answer

Add texts here. Do not delete this text first.

This page titled 5.2: Proving Set Relationships is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

5.3: Properties of Set Operations

PREVIEW ACTIVITY 5.3.1: Exploring a Relationship between Two Sets

Let A and B be subsets of some universal set U.

1. Draw two general Venn diagrams for the sets A and B. On one, shade the region that represents $(A \cup B)^c$, and on the other, shade the region that represents $A^c \cap B^c$. Explain carefully how you determined these regions.
2. Based on the Venn diagrams in Part (1), what appears to be the relationship between the sets ((A \cup B)^c\) and $A^c \cap B^c$?

Some of the properties of set operations are closely related to some of the logical operators we studied in Section 2.1. This is due to the fact that set intersection is defined using a conjunction (and), and set union is defined using a disjunction (or). For example, if A and B are subsets of some universal set U, then an element x is in $A \cup B$ if and only if $x \in A$ or $x \in B$.

3. Use one of De Morgan's Laws (Theorem 2.8 on page 48) to explain carefully what it means to say that an element x is not in $A \cup B$.
4. What does it mean to say that an element x is in A^c? What does it mean to say that an element x is in B^c?
5. Explain carefully what it means to say that an element x is in $A^c \cap B^c$.
6. Compare your response in Part (3) to your response in Part (5). Are they equivalent? Explain.
7. How do you think the sets $(A \cup B)^c$ and $A^c \cap B^c$ are related? Is this consistent with the Venn diagrams from Part (1)?

PREVIEW ACTIVITY 5.3.2: Proving that Statements Are Equivalent

1. Let X, Y, and Z be statements. Complete a truth table for
   $[(X \to Y) \wedge (Y \to Z)] \to (X \to Z)$.
2. Assume that P, Q, and R are statements and that we have proven that the following conditional statements are true:

   - If P then $Q (P \to Q)$.
   - If R then $P (R \to P)$.
   - If Q then $R (Q \to R)$.

   Explain why each of the following statements is true.

   (a) P if and only if $Q (P \leftrightarrow Q$.
   (b) Q if and only if $R (Q \leftrightarrow R$.
   (c) R if and only if $P (R \leftrightarrow P$.
   Remember that $X \leftrightarrow Y$ is logically equivalent to $(X \to Y) \wedge (Y \to X)$.

Algebra of Sets – Part 1

This section contains many results concerning the properties of the set operations. We have already proved some of the results. Others will be proved in this section or in the exercises. The primary purpose of this section is to have in one place many of the properties of set operations that we may use in later proofs. These results are part of what is known as the **algebra of sets** or as **set theory**.

Theorem 5.17

Let A, B, and C be subsets of some universal set U. Then

- $A \cap B \subseteq A$ and $A \subseteq A \cup B$.
- If $A \subseteq B$, then $A \cap C \subseteq B \cap C$ and $A \cup C \subseteq B \cup C$.

Proof

The first part of this theorem was included in Exercise (7) from Section 5.2. The second part of the theorem was Exercise (12) from Section 5.2.

The next theorem provides many of the properties of set operations dealing with intersection and union. Many of these results may be intuitively obvious, but to be complete in the development of set theory, we should prove all of them. We choose to prove only some of them and leave some as exercises.

Theorem 5.18: Algebra of Set Operations

Let A, B, and C be subsets of some universal set U. Then all of the following equalities hold.

Proporties of the Empty Set $A \cap \emptyset = \emptyset$ $A \cap U = A$ and the Universal Set $A \cup \emptyset = A$ $A \cup U = U$

Idempotent Laws $A \cap A = A$ $A \cup A = A$

Commutative Laws $A \cap B = B \cap A$ $A \cup B = B \cup A$

Associative Laws $(A \cap B) \cap C = A \cap (B \cap C)$
$(A \cup B) \cup C = A \cup (B \cup C)$

Distributive Laws $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Before proving some of these properties, we note that in Section 5.2, we learned that we can prove that two sets are equal by proving that each one is a subset of the other one. However, we also know that if S and T are both subsets of a universal set U, then

$S = T$ if and only if for each $x \in U$, $x \in S$ if and only if $x \in T$.

We can use this to prove that two sets are equal by choosing an element from one set and chasing the element to the other set through a sequence of “if and only if” statements. We now use this idea to prove one of the commutative laws.

Proof of One of the Commutative Laws in Theorem 5.18

We will prove that $A \cap B = B \cap A$. Let $x \in A \cap B$. Then

$$x \in A \cap B \text{ if and only if } x \in A \text{ and } x \in B. \tag{5.3.1}$$

However, we know that if P and Q are statements, then $PwedgeQ$ is logically equivalent to $Q \wedge P$. Consequently, we can conclude that

$$x \in A \text{ and } x \in B \text{ if and only if } x \in B \text{ and } x \in A. \tag{5.3.2}$$

Now we know that

$$x \in B \text{ and } x \in A \text{ if and only if } x \in B \cap A. \tag{5.3.3}$$

This means that we can use (5.3.1), (5.3.2) and (5.3.3) to conclude that

$$x \in A \cap B \text{ if and only if } x \in B \cap A,$$

and, hence, we have proved that $A \cap B = B \cap A$.

□

Progress Check 5.19: Exploring a Distributive Property

We can use Venn diagrams to explore the more complicated properties in Theorem 5.18, such as the associative and distributive laws. To that end, let A, B, and C be subsets of some universal set U.

1. Draw two general Venn diagrams for the sets A, B, and C. On one, shade the region that represents $A \cup (B \cap C$, and on the other, shade the region that represents $(A \cup B) \cap (A \cup C)$. Explain carefully how you determined these regions.
2. Based on the Venn diagrams in Part (1), what appears to be the relationship between the sets $A \cup (B \cap C$ and $(A \cup B) \cap (A \cup C)$?

Answer

Add texts here. Do not delete this text first.

Proof of One of the Distributive Laws in Theorem 5.18

We will now prove the distributive law explored in Progress Check 5.19. Notice that we will prove two subset relations, and that for each subset relation, we will begin by choosing an arbitrary element from a set. Also notice how nicely a proof dealing with the union of two sets can be broken into cases.

Proof. Let A, B, and C be subsets of some universal set U. We will prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ by proving that each set is a subset of the other set.

We will first prove that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C$. We let $x \in A \cup (B \cap C)$. Then $x \in A$ or $x \in B \cap C$.

So in one case, if $x \in A$, then $x \in A \cup B$ and $x \in A \cup C$. This means that $x \in (A \cup B) \cap (A \cup C)$.

On the other hand, if $x \in B \cap C$, then $x \in B$ and $x \in C$. But $x \in B$ implies that $x \in A \cup B$, and $x \in C$ implies that $x \in A \cup C$. Since x is in both sets, e conclude that $x \in (A \cup B) \cap (A \cup C)$. So in both cases, we see that $x \in (A \cup B) \cap (A \cup C)$, and this proves that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C$.

We next prove that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. So let $y \in (A \cup B) \cap (A \cup C)$. Then, $y \in A \cup B$ and $y \in A \cup C$. We must prove that $y \in A \cup (B \cap C)$. We will consider the two cases where $y \in A$ or $y \notin A$. In the case where $y \in A$, we see that $y \in A \cup (B \cap C)$.

So we consider the case that $y \notin A$. It has been established that $y \in A \cup B$ and $y \in A \cup C$. Since $y \not in A$ and $y \in A \cup B$, y must be an element of B. Similarly, since $y \notin A$ and $y \in A \cup C$, y must be an element of C. Thus, $y \in B \cap C$ and, hence, $y \in A \cup (B \cap C)$.

In both cases, we have proved that $y \in A \cup (B \cap C)$. This proves that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. The two subset relations establish the equality of the two sets. Thus, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

$square$

Important Properties of Set Complements

The three main set operations are union, intersection, and complementation. The- orems 5.18 and 5.17 deal with properties of unions and intersections. The next theorem states some basic properties of complements and the important relations dealing with complements of unions and complements of intersections. Two relationships in the next theorem are known as **De Morgan's Laws** for sets and are closely related to De Morgan's Laws for statements.

Theorem 5.20

Let A, B, and C be subsets of some universal set U. Then the following are true:

Basic Properties $(A^c)^c = A$
$A - B = A \cap B^c$

Empty Set and Universal Set $A - \emptyset = A$ and $A - U = \emptyset$
$\emptyset^c = U$ and $U^c = \emptyset$

De Morgan's Laws $(A \cap B)^c = A^c \cup B^c$
$(A \cup B)^c = A^c \cap B^c$

Subsets and Complements $A \subseteq B$ if and only if $B^c \subseteq A^c$

Proof

We will only prove one of De Morgan's Laws, namely, the one that was explored in Preview Activity $5.3.1$. The proofs of the other parts are left as exercises. Let A and B be subsets of some universal set U. We will prove that $(A \cup B)^c = A^c \cap B^c$ by proving that an element is in $(A \cup B)^c$ if and only if it is in $A^c \cap B^c$. So let x be in the universal set U. Then

$$x \in (A \cup B)^c \text{ if and only if } x \notin A \cup B. \tag{5.3.4}$$

and

$$x \notin A \cup B \text{ if and only if } x \notin A \text{ and } x \notin B. \tag{5.3.5}$$

Combining (5.3.4) and (5.3.5), we see that

$$x \in (A \cup B)^c \text{ if and only if } x \notin A \text{ and } x \notin B. \tag{5.3.6}$$

In addition, we know that

$$x \notin A \text{ and } x \notin B \text{ if and only if } x \in A^c \text{ and } x \in B^c. \tag{5.3.7}$$

and this is true if and only if $x \in A^c \cap B^c$. So we can use (5.3.6) and (5.3.7) to conclude that

$x \in (A \cup B)^c$ if and only if $x \in A^c \cap B^c$.

and, hence, that $(A \cup B)^c = A^c \cap B^c$.

□

? Progress Check 5.21: Using the Algebra of Sets

1. Draw two general Venn diagrams for the sets A, B, and C. On one, shade the region that represents $(A \cup B) - C$, and on the other, shade the region that represents $(A - C) \cup (B - C)$. Explain carefully how you determined these regions and why they indicate that $(A \cup B) - C = (A - C) \cup (B - C)$.

It is possible to prove the relationship suggested in Part (1) by proving that each set is a subset of the other set. However, the results in Theorems 5.18 and 5.20 can be used to prove other results about set operations. When we do this, we say that we are using the algebra of sets to prove the result. For example, we can start by using one of the basic properties in Theorem 5.20 to write

$$A \cup B) - C = (A \cup B) \cap C^c.$$

We can then use one of the commutative properties to write

$$\begin{aligned} (A \cup B) - C &= (A \cup B) \cap C^c \\ &= C^c \cap (A \cup B). \end{aligned} \tag{5.3.8}$$

2. Determine which properties from Theorems 5.18 and 5.20 justify each of the last three steps in the following outline of the proof that $(A \cup B) - C = (A - C) \cup (B - C)$.

$$\begin{aligned} (A \cup B) - C &= (A \cup B) \cap C^c && \text{(Theorem 5.20)} \\ &= C^c \cap (A \cup B) && \text{(Commutative Property)} \\ &= (C^c \cap A) \cup (C^c \cap B) \\ &= (A \cap C^c) \cup (B \cap C^c) \\ &= (A - C) \cup (B - C) \end{aligned} \tag{5.3.9}$$

Note: It is sometimes difficult to use the properties in the theorems when the theorems use the same letters to represent the sets as those being used in the current problem. For example, one of the distributive properties from Theorems 5.18 can be written as follows: For all sets X, Y, and Z that are subsets of a universal set U,

$$(X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z).$$

Answer

Add texts here. Do not delete this text first.

Proving that Statements Are Equivalent

When we have a list of three statements P , Q, and R such that each statement in the list is equivalent to the other two statements in the list, we say that the three statements are equivalent. This means that each of the statements in the list implies each of the other statements in the list.

The purpose of Preview Activity $5.3.2$ was to provide one way to prove that three (or more) statements are equivalent. The basic idea is to prove a sequence of conditional statements so that there is an unbroken chain of conditional statements from each statement to every other statement. This method of proof will be used in Theorem 5.22.

Theorem 5.22

Let A and B be subsets of some universal set U. The following are equivalent:

1. $A \subseteq B$
2. $A \cap B^c = \emptyset$
3. $A^c \cup B = U$

Proof

To prove that these are equivalent conditions, we will prove that (1) implies (2), that (2) implies (3), and that (3) implies (1).

Let A and B be subsets of some universal set U. We have proved that (1) implies (2) in Proposition 5.14.

To prove that (2) implies (3), we will assume that $A \cap B^c = \emptyset$ and use the fact that $\emptyset^c = U$. We then see that

$(A \cap B^c)^c = \emptyset^c$.

Then, using one of De Morgan's Laws, we obtain

Misplaced &

This completes the proof that (2) implies (3).

We now need to prove that (3) implies (1). We assume that $A^c \cup B = U$ and will prove that $A \subseteq B$ by proving that every element of A must be in B.

So let $x \in A$. Then we know that $x \notin A^c$. However, $x \in U$ and since $A^c \cup B = U$, we can conclude that $x \in A^c \cup B$. Since $x \notin A^c$, we conclude that $x \in B$. This proves that $A \subseteq B$ and hence that (3) implies (1).

Since we have now proved that (1) implies (2), that (2) implies (3), and that (3) implies (1), we have proved that the three conditions are equivalent.

? Exercises for Section 5.3

1. Let A be a subset of some universal set U. Prove each of the following (from Theorem 5.20):

   (a) $(A^c)^c = A$
   (b) $A - \emptyset = A$
   (c) $\emptyset^c = U$
   (d) $U^c = \emptyset$
2. Let A, B, and C be subsets of some universal set U. As part of Theorem 5.18, we proved one of the distributive laws. Prove the other one. That is, prove that
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \tag{5.3.10}$$
3. Let A, B, and C be subsets of some universal set U. As part of Theorem 5.20, we proved one of De Morgan’s Laws. Prove the other one. That is, prove that
$$(A \cap B)^c = A^c \cup B^c. \tag{5.3.11}$$
4. Let A, B, and C be subsets of some universal set U.

   (a) Draw two general Venn diagrams for the sets A, B, and C. On one, shade the region that represents $A - (B \cup C)$, and on the other, shade the region that represents $(A - B) \cap (A - C)$. Based on the Venn diagrams, make a conjecture about the relationship between the sets $A - (B \cup C)$ and $(A - B) \cap (A - C)$.
   (b) Use the choose-an-element method to prove the conjecture from Exercise (4a).
   (c) Use the algebra of sets to prove the conjecture from Exercise (4a).

5. Let A, B, and C be subsets of some universal set U.

   (a) Draw two general Venn diagrams for the sets A, B, and C. On one, shade the region that represents $A-(B\cap C)$, and on the other, shade the region that represents $(A-B)\cup(A-C)$. Based on the Venn diagrams, make a conjecture about the relationship between the sets $A-(B\cap C)$ and $(A-B)\cup(A-C)$.
   (b) Use the choose-an-element method to prove the conjecture from Exercise (5a).
   (c) Use the algebra of sets to prove the conjecture from Exercise (5a).
6. Let A, B, and C be subsets of some universal set U. Prove or disprove each of the following:

   (a) $(A\cap B)-C=(A-C)\cap(B-C)$
   (b) $(A\cup B)-(A\cap B)=(A-B)\cup(B-A)$
7. Let A, B, and C be subsets of some universal set U.

   (a) Draw two general Venn diagrams for the sets A, B, and C. On one, shade the region that represents $A-(B-C)$, and on the other, shade the region that represents $(A-B)-C$. Based on the Venn diagrams, make a conjecture about the relationship between the sets $A-(B-C)$ and $(A-B)-C$.
   (b) Prove the conjecture from Exercise (7a).
8. Let A, B, and C be subsets of some universal set U.

   (a) Draw two general Venn diagrams for the sets A, B, and C. On one, shade the region that represents $A-(B-C)$, and on the other, shade the region that represents $(A-B)\cup(A-C^c)$. Based on the Venn diagrams, make a conjecture about the relationship between the sets $A-(B-C)$ and $(A-B)\cup(A-C^c)$.
   (b) Prove the conjecture from Exercise (8a).
9. Let A and B be subsets of some universal set U.

   (a) Prove that A and $B-A$ are disjoint sets.
   (b) Prove that $A\cup B=A\cup(B-A)$.
10. Let A and B be subsets of some universal set U.

    (a) Prove that $A-B$ and $A\cap B$ are disjoint sets.
    (b) Prove that $A=(A-B)\cup(A\cap B)$.
11. Let A and B be subsets of some universal set U. Prove or disprove each of the following:

    (a) $A-(A\cap B^c)=A\cap B$
    (b) $(A^c\cup B)^c\cap A=A-B$
    (c) $(A\cup B)-A=B-A$
    (d) $(A\cup B)-B=A-(A\cap B)$
    (e) $(A\cup B)-(A\cap B)=(A-B)\cup(B-A)$
12. **Evaluation of proofs**
    See the instructions for Exercise (19) on page 100 from Section 3.1.

(a)

Let A, B, and C be subsets of some universal set U, then $A-(B-C)=A-(B\cup C)$.

Proof

$$\begin{aligned} A-(B-C) &= (A-B)-(A-C)\\ &= (A\cap B^c)\cap(A\cap C^c)\\ &= A\cap(B^c\cap C^c)\\ &= A\cap(B\cup C)^c\\ &= A-(B\cup C)\end{aligned} \tag{5.3.12}$$

Theorem 5.3.1

Let A, B, and C be subsets of some universal set U, then $A-(B\cup C)=(A-B)\cap(A-C)$.

Proof

We first write $A-(B\cup C)=A\cap(B\cup C)^c$ and then use one of De Morgan's Laws to obtain

$$A-(B\cup C)=A\cap(B^c\cap C^c).$$

We now use the fact that $A=A\cap A$ and obtain

$$\begin{aligned} A-(B\cup C) &= A\cap A\cap B^c\cap C^c \\ &= (A\cap B^c)\cap(A\cap C^c) \\ &= (A-B)\cap(A-C). \end{aligned} \tag{5.3.13}$$

Explorations and Activities

13. **(Comparison to Properties of the Real Numbers).** The following are some of the basic properties of addition and multiplication of real numbers

Commutative Laws: $a+b=b+a$, for all $a,b\in\mathbb{R}$.
$a\cdot b=b\cdot a$, for all $a,b\in\mathbb{R}$.

Associative Laws: $(a+b)+c=a+(b+c)$, for all $a,b,c\in\mathbb{R}$.
$(a\cdot b)\cdot c=a\cdot(b\cdot c)$, for all $a,b,c\in\mathbb{R}$.

Distributive Law: $a\cdot(b+c)=a\cdot b+a\cdot c$, for all $a,b,c\in\mathbb{R}$.

Additive Identity: For all $a\in\mathbb{R}$, $a+0=a=0+a$.

Multiplicative Identity: For all $a\in\mathbb{R}$, $a\cdot 1=a=1\cdot a$.

Additive Inverses: For all $a\in\mathbb{R}$, $a+(-a)=0=(-a)+a$.

Multiplicative Inverses: For all $a\in\mathbb{R}$ with $a\neq 0$, $a\cdot a^{-1}=1=a^{-1}\cdot a$.

Discuss the similarities and differences among the properties of addition and multiplication of real numbers and the properties of union and intersection of sets.

Answer

Add texts here. Do not delete this text first.

This page titled 5.3: Properties of Set Operations is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

5.4: Cartesian Products

? PREVIEW ACTIVITY $5.4.1$: An Equation with Two Variables

In Section 2.3, we introduced the concept of the **truth set of an open sentence with one variable**. This was defined to be the set of all elements in the universal set that can be substituted for the variable to make the open sentence a true statement.

In previous mathematics courses, we have also had experience with open sentences with two variables. For example, if we assume that x and y represent real numbers, then the equation

$$2x+3y=12$$

is an open sentence with two variables. An element of the truth set of this open sentence (also called a solution of the equation) is an ordered pair (a, b) of real numbers so that when a is substituted for x and b is substituted for y, the open sentence becomes a true statement (a true equation in this case). For example, we see that the ordered pair (6, 0) is in the truth set for this open sentence since

$$2\cdot 6+3=12$$

is a true statement. On the other hand, the ordered pair (4, 1) is not in the truth set for this open sentence since

$$2\cdot 4+3\cdot 1=12$$

is a false statement.

Important Note: The order of the of the two numbers in the ordered pair is very important. We are using the convention that the first number is to be substituted for x and the second number is to be substituted for y. With this convention, (3, 2) is a solution of the equation $2x+3y=12$, but (2, 3) is not a solution of this equation.

1. List six different elements of the truth set (often called the solution set) of the open sentence with two variables $2x+3y=12$.
2. From previous mathematics courses, we know that the graph of the equation $2x+3y=12$ is a straight line. Sketch the graph of the equation $2x+3y=12$ in the xy-coordinate plane. What does the graph of the equation $2x+3y=12$ show?
3. Write a description of the solution set S of the equation $2x+3y=12$ using set builder notation.

? PREVIEW ACTIVITY $5.4.1$: The Cartesian Product of Two Sets

In Preview Activity $5.4.1$, we worked with ordered pairs without providing a formal definition of an ordered pair. We instead relied on your previous work with ordered pairs, primarily from graphing equations with two variables. Following is a formal definition of an ordered pair.

Definition: ordered pair

Let A and B be sets. An *ordered pair* (with first element from A and second element from B) is a single pair of objects, denoted by (a, b), with $a\in A$ and $b\in B$ and an implied order. This means that for two ordered pairs to be equal, they must contain exactly the same objects in the same order. That is, if $a,c\in A$ and $b,d\in B$, then

(a, b) = (c, d) if and only if $a=c$ and $b=d$.

The objects in the ordered pair are called the *coordinates* of the ordered pair. In the ordered pair (a, b), a is the *first coordinate* and b is the *second coordinate*.

We will now introduce a new set operation that gives a way of combining elements from two given sets to form ordered pairs. The basic idea is that we will create a set of ordered pairs.

Definition: Cartesian product

If A and B are sets, then the *Cartesian product*, $A\times B$, of A and B is the set of all ordered pairs (x, y) where $x\in A$ and $y\in B$. We use the notation $A\times B$ for the Cartesian product of A and B, and using set builder notation, we can write

$$A\times B=\{(x,y)\mid x\in A \text{ and } y\in B\}.$$

We frequently read $A \times B$ as "A cross B." In the case where the two sets are the same, we will write A^2 for $A \times A$. That is,

$$A^2 = A \times A = \{(a, b) \mid a \in A \text{ and } b \in A\}.$$

Let $A = \{1, 2, 3\}$ and $B = \{a, b\}$.

1. Is the ordered pair $(3, a)$ in the Cartesian product $A \times B$? Explain.
2. Is the ordered pair $(3, a)$ in the Cartesian product $A \times A$? Explain.
3. Is the ordered pair $(3, 1)$ in the Cartesian product $A \times A$? Explain.
4. Using the roster method to specify all the elements of $A \times B$. (Remember that the elements of $A \times B$ will be ordered pairs.
5. Use the roster method to specify all of the elements of the set $A \times A = A^2$.
6. For any sets C and D, explain carefully what it means to say that the ordered pair (x, y) is not in the Cartesian product $C \times D$.

Cartesian Products

When working with Cartesian products, it is important to remember that the Cartesian product of two sets is itself a set. As a set, it consists of a collection of elements. In this case, the elements of a Cartesian product are ordered pairs. We should think of an ordered pair as a single object that consists of two other objects in a specified order. For example,

- If $a \neq 1$, then the ordered pair $(1, a)$ is not equal to the ordered pair $(a, 1)$. That is, $(1, a) \neq (a, 1)$.
- If $A = \{1, 2, 3\}$ and $B = \{a, b\}$, then the ordered pair $(3, a)$ is an element of the set $A \times B$. That is, $(3, a) \in A \times B$.
- If $A = \{1, 2, 3\}$ and $B = \{a, b\}$, then the ordered pair $(5, a)$ is not an element of the set $A \times B$ since $5 \notin A$. That is, $(5, a) \notin A \times B$.

In Section 5.3, we studied certain properties of set union, set intersection, and set complements, which we called the algebra of sets. We will now begin something similar for Cartesian products. We begin by examining some specific examples in Progress Check 5.23 and a little later in Progress Check 5.24.

? progress check 5.23 (relationships between Cartesian products)

Let $A = \{1, 2, 3\}$, $T = \{\text{a, b}\}$, and $C = \{\text{a, c}\}$. We can then form new sets from all of the set operations we have studied. For example, $B \cap C = \{a\}$, and so

$$A \times (B \cap C) = \{(1, a), (2, a), (3, a)\}.$$

1. Use the roster method to list all of the elements (ordered pairs) in each of the following sets:

   (a) $A \times B$
   (b) $T \times B$
   (c) $A \times C$
   (d) $A \times (B \cap C)$
   (e) $(A \times B) \cap (A \times C)$
   (f) $A \times (B \cup C)$
   (g) $(A \times B) \cup (A \times C)$
   (h) $A \times (B - C)$
   (i) $(A \times B) - (A \times C)$
   (j) $B \times A$
2. List all the relationships between the sets in Part (1) that you observe.

Answer

Add texts here. Do not delete this text first.

The Cartesian Plane

In Preview Activity $5.4.1$, we sketched the graph of the equation $2x + 3y = 12$ in the xy-plane. This xy-plane, with which you are familiar, is a representation of the set $\mathbb{R} \times \mathbb{R}$ or $\mathbb{R}^2$. This plane is called the *Cartesian plane*.

The basic idea is that each ordered pair of real numbers corresponds to a point in the plane, and each point in the plane corresponds to an ordered pair of real numbers. This geometric representation of $\mathbb{R}^2$ is an extension of the geometric representation of $\mathbb{R}$ as a straight line whose points correspond to real numbers.

Since the Cartesian product $\mathbb{R}^2$ corresponds to the Cartesian plane, the Cartesian product of two subsets of $\mathbb{R}$ corresponds to a subset of the Cartesian plane. For example, if A is the interval [1, 3], and B is the interval [2, 5], then

$$A \times B = \{(x, y) \in \mathbb{R}^2 \mid 1 \le x \le 3 \text{ and } 2 \le y \le 5\}.$$

A graph of the set $A \times B$ can then be drawn in the Cartesian plane as shown in Figure 5.6.

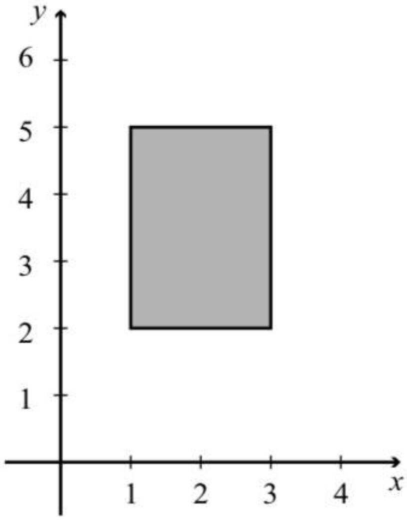


Figure 5.6: Cartesian Product $A \times B$

This illustrates that the graph of a Cartesian product of two intervals of finite length in $\mathbb{R}$ corresponds to the interior of a rectangle and possibly some or all of its boundary. The solid line for the boundary in Figure 5.6 indicates that the boundary is included. In this case, the Cartesian product contained all of the boundary of the rectangle. When the graph does not contain a portion of the boundary, we usually draw that portion of the boundary with a dotted line.

Note: A Caution about Notation. The standard notation for an open interval in $\mathbb{R}$ is the same as the notation for an ordered pair, which is an element of $\mathbb{R} \times \mathbb{R}$. We need to use the context in which the notation is used to determine which interpretation is intended. For example,

- If we write $(sqrt2, 7) \in \mathbb{R} \times \mathbb{R}$, then we are using $(sqrt2, 7)$ to represent an ordered pair of real numbers.
- If we write $(1, 2) \times \{4\}$, then we are interpreting (1, 2) as an open interval. We could write

$$(1, 2) \times \{4\} = \{(x, 4) \mid 1 < x < 2\}.$$

The following progress check explores some of the same ideas explored in Progress Check 5.23 except that intervals of real numbers are used for the sets.

? Progress Check 5.24: Cartesian Products of Intervals

We will use the following intervals that are subsets of $\mathbb{R}$.

$$A = [0, 2]\ T = (1, 2)\ B = [2, 4)\ C = (3, 5]$$

1. Draw a graph of each of the following subsets of the Cartesian plane and write each subset using set builder notation.

   (a) $A \times B$
   (b) $T \times B$
   (c) $A \times C$

   (d) $A \times (B \cap C)$
   (e) $(A \times B) \cap (A \times C)$
   (f) $A \times (B \cup C)$
   (g) $(A \times B) \cup (A \times C)$
   (h) $A \times (B - C)$
   (i) $(A \times B) - (A \times C)$
   (j) $B \times A$
2. List all the relationships between the sets in Part (1) that you observe.

Answer

Add texts here. Do not delete this text first.

One purpose of the work in Progress Checks 5.23 and 5.24 was to indicate the plausibility of many of the results contained in the next theorem.

Theorem 5.25

Let A, B. and C be sets. Then

1. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
3. $(A \cap B) \times C = (A \times C) \cap (B \times C)$
4. $(A \cup B) \times C = (A \times C) \cup (B \times C)$
5. $A \times (B - C) = (A \times B) - (A \times C)$
6. $(A - B) \times C = (A \times C) - (B \times C)$
7. If $T \subseteq A$, then $T \times B \subseteq A \times B$.
8. If $T \subseteq B$, then $A \times Y \subseteq A \times B$.

We will not prove all these results; rather, we will prove Part (2) of Theorem 5.25 and leave some of the rest to the exercises. In constructing these proofs, we need to keep in mind that Cartesian products are sets, and so we follow many of the same principles to prove set relationships that were introduced in Sections 5.2and 5.3.

The other thing to remember is that the elements of a Cartesian product are ordered pairs. So when we start a proof of a result such as Part (2) of Theorem 5.25, the primary goal is to prove that the two sets are equal. We will do this by proving that each one is a subset of the other one. So if we want to prove that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$, we can start by choosing an arbitrary element of $A \times (B \cup C)$. The goal is then to show that this element must be in $(A \times B) \cup (A \times C)$. When we start by choosing an arbitrary element of $A \times (B \cup C)$, we could give that element a name. For example, we could start by letting

$$u \text{ be an element of } A \times (B \cup C). \tag{5.4.1}$$

We can then use the definition of "ordered pair" to conclude that

$$\text{there exists } x \in A \text{ and there exits } y \in B \cup C \text{ such that } u = (x, y). \tag{5.4.2}$$

In order to prove that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$, we must now show that the ordered pair u from (5.4.1) is in $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$. In order to do this, we can use the definition of set union and prove that

$$u \in (A \times B) \text{ or } u \in (A \times C). \tag{5.4.3}$$

Since $u = (x, y)$, we can prove (5.4.3) by proving that

$$(x \in A \text{ and } y \in B) \text{ or } (x \in A \text{ and } y \in C). \tag{5.4.4}$$

If we look at the sentences in (5.4.2) and (5.4.4), it would seem that we are very close to proving that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$. Following is a proof of Part (2) of Theorem 5.25.

Theorem 5.25 (Part (2)).

Let A, B. and C be sets. Then

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

Proof

Let A, B. and C be sets. We will prove that $A \times (B \cup C)$ is equal to $(A \times B) \cup (A \times C)$ by proving that each set is a subset of the other set.

To prove that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$, we let $u \in A \times (B \cup C)$. Then there exists $x \in A$ and there exists $y \in B \cup C$ such that $u = (x, y)$. Since $y \in B \cup C$, we know that $y \in B$ or $y \in C$.

In the case where $y \in B$, we have $u = (x, y)$, where $x \in A$ and $y \in B$. So in this case, $u \in A \times B$, and hence $u \in (A \times B) \cup (A \times C)$. Similarly, in the case where $y \in C$, we have $u = (x, y)$, where $x \in A$ and $y \in C$. So in this case, $u \in A \times C$ and, hence, $u \in (A \times B) \cup (A \times C)$.

In both cases, $u \in (A \times B) \cup (A \times C)$. Hence, we may conclude that if u is an element of $A \times (B \cup C)$, then $u \in (A \times B) \cup (A \times C)$, and this proves that

$$A \times (B \cup C) \subseteq (A \times B) \cup (A \times C). \tag{5.4.5}$$

We must now prove that $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$. So we let $v \in (A \times B) \cup (A \times C)$. Then $v \in (A \times B)$ or $v \in (A \times C)$.

In the case where $v \in (A \times B)$, we know that there exists $s \in A$ and there exists $t \in B$ such that $v = (s, t)$. But because $t \in C$, we can conclude that $t \in B \cup C$ and, hence, $v \in A \times (B \cup C)$.

In both cases, $v \in A \times (B \cup C)$. Hence, we may conclude that if $v \in (A \times B) \cup (A \times C)$, then $v \in A \times (B \cup C)$, and this proves that

$$(A \times B) \cup (A \times C) \subseteq A \times (B \cup C). \tag{5.4.6}$$

The relationships in (5.4.5) and (5.4.6) prove that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Final Note.

The definition of an ordered pair in Preview Activity 5.4.2 may have seemed like a lengthy definition, but in some areas of mathematics, an even more formal and precise definition of “ordered pair” is needed. This definition is explored in Exercise (10).

Exercises for Section 5.4

1. Let $A = \{1, 2\}$, $B = \{a, b, c, d\}$, and $C = \{1, a, b\}$. Use the roster method to list all of the elements of each of the following sets:

   (a) $A \times B$
   (b) $B \times A$
   (c) $A \times C$
   (d) A^2
   (e) $A \times (B \cap C)$
   (f) $(A \times B) \cap (A \times C)$
   (g) $A \times \emptyset$
   (h) $B \times \{2\}$
2. Sketch a graph of each of the following Cartesian products in the Cartesian plane.

   (a) $[0, 2] \times [1, 3]$
   (b) $(0, 2) \times (1, 3]$

(c) [2, 3] × {1}
(d) {1} × [2, 3]
(e) ℝ × (2, 4)
(f) (2, 4) × ℝ
(g) ℝ × {-1}
(h) {-1} × [1, +∞)

3. Prove Theorem 5.25, Part (1): $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
4. Prove Theorem 5.25, Part (4): $(A \cup B) \times C = (A \times C) \cup (B \times C)$.
5. Prove Theorem 5.25, Part (5): $A \times (B - C) = (A \times B) - (A \times C)$.
6. Prove Theorem 5.25, Part (7): If $T \subseteq A$, then $T \times B \subseteq A \times B$.
7. Let $A = \{1\}$, $B = \{2\}$, and $C = \{3\}$.

   (a) Explain why $A \times B \neq B \times A$.
   (b) Explain why $A \times B) \times C \neq A \times (B \times C)$.
8. Let A and B be nonempty sets. Prove that $A \times B = B \times A$ if and only if $A = B$.
9. Is the following proposition true or false? Justify your conclusion.

   Let A, B and C be sets with $A \neq \emptyset$. If $A \times B = A \times C$, then $B = C$. Explain where the assumption that $A \neq \emptyset$ is needed.

   Explorations and Activities
10. **(A Set Theoretic Definition of an Ordered Pair)** In elementary mathematics, the notion of an ordered pair introduced at the beginning of this section will suffice. However, if we are interested in a formal development of the Cartesian product of two sets, we need a more precise definition of ordered pair. Following is one way to do this in terms of sets. This definition is credited to Kazimierz Kuratowski (1896 – 1980). Kuratowski was a famous Polish mathematician whose main work was in the areas of topology and set theory. He was appointed the Director of the Polish Academy of Sciences and served in that position for 19 years.

    Let x be an element of the set A, and let y be an element of the set B. The **ordered pair** (x, y) is defined to be the set $\{\{x\},\{x,y\}\}$. That is,

    $$(x,y) = \{\{x\},\{x,y\}\}. \tag{5.4.7}$$

    (a) Explain how this definition allows us to distinguish between the ordered pairs (3, 5) and (5, 3).

    (b) Let A and B be sets and let $a, c \in A$ and $b, d \in B$. Use this definition of an ordered pair and the concept of set equality to prove that $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

    An ordered triple can be thought of as a single triple of objects, denoted by (a, b, c), with an implied order. This means that in order for two ordered triples to be equal, they must contain exactly the same objects in the same order. That is $(a, b, c) = (p, q, r)$ if and only if $a = p$, $b = q$ and $c = r$.

    (c) Let A, B and C be sets, and let $x \in A$, $y \in B$, and $z \in C$. Write a set theoretic definition of the ordered triple (x, y, z) similar to the set theoretic definition of "ordered pair."

Answer

Add texts here. Do not delete this text first.

This page titled 5.4: Cartesian Products is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

5.5: Indexed Families of Sets

Preview Activity 5.5.1: The Union and Intersection of a Family of Sets

In Section 5.3, we discussed various properties of set operations. We will now focus on the associative properties for set union and set intersection. Notice that the definition of "set union" tells us how to form the union of two sets. It is the associative law that allows us to discuss the union of three sets. Using the associate law, if A, B, and C are subsets of some universal set, then we can define $A \cup B \cup C$ to be $(A \cup B) \cup C$ or $A \cup (B \cup C)$. That is,

$$A \cup B \cup C = (A \cup B) \cup C = A \cup (B \cup C).$$

For this activity, the universal set is N and we will use the following four sets:

$$A = \{1, 2, 3, 4, 5\}$$

$$B = \{2, 3, 4, 5, 6\}$$

$$C = \{3, 4, 5, 6, 7\}$$

$$D = \{4, 5, 6, 7, 8\}$$

1. Use the roster method to specify the sets $A \cup B \cup C$, $B \cup C \cup D$, $A \cap B \cap C$, and $B \cap C \cap D$.
2. Use the roster method to specify each of the following sets. In each case, be sure to follow the order specified by the parentheses.

   (a) $(A \cup B \cup C) \cup D$
   (b) $A \cup (B \cup C \cup D)$
   (c) $A \cup (B \cup C) \cup D$
   (d) $(A \cup B) \cup (C \cup D)$
   (e) $(A \cap B \cap C) \cap D$
   (f) $A \cap (B \cap C \cap D)$
   (g) $A \cap (B \cap C) \cap D$
   (h) $(A \cap B) \cap (C \cap D)$
3. Based on the work in Part (2), does the placement of the parentheses matter when determining the union (or intersection) of these four sets? Does this make it possible to define $A \cup B \cup C \cup D$ and $A \cap B \cap C \cap D$?

We have already seen that the elements of a set may themselves be sets. For example, the power set of a set T, $\mathcal{P}(T)$, is the set of all subsets of T. The phrase, "a set of sets" sounds confusing, and so we often use the terms ***collection*** and ***family*** when we wish to emphasize that the elements of a given set are themselves sets. We would then say that the power set of T is the family (or collection) of sets that are subsets of T.

One of the purposes of the work we have done so far in this preview activity was to show that it is possible to define the union and intersection of a family of sets.

Definition

Let $\mathcal{C}$ be a family of sets. The **union over** $\mathcal{C}$ is defined as the set of all elements that are in at least one of the sets in $\mathcal{C}$. We write

$$\bigcup_{X \in \mathcal{C}} X = \{x \in U \mid x \in X \text{ for some } X \in \mathcal{C}\}$$

The **intersection over** $\mathcal{C}$ is defined as the set of all elements that are in all of the sets in $\mathcal{C}$. That is,

$$\bigcap_{X \in \mathcal{C}} X = \{x \in U \mid x \in X \text{ for some } X \in \mathcal{C}\}$$

For example, consider the four sets A, B, C, and D used earlier in this preview activity and the sets

$$S = \{5, 6, 7, 8, 9\} \text{ and } T = \{6, 7, 8, 9, 10\}$$

We can then consider the following families of sets: $\mathcal{A} = \{A, B, C, D\}$ and $\mathcal{B} = \{A, B, C, D, S, T\}$

4. Explain why

$\bigcup_{X\in\mathcal{A}} X = A\cup B\cup C\cup D$ and $\bigcap_{X\in\mathcal{A}} X = A\cap B\cap C\cap D$

and use your work in (1), (2), and (3) to determine $\bigcup_{X\in\mathcal{A}} X$ and $\bigcap_{X\in\mathcal{A}} X$.

5. Use the roster method to specify $\bigcup_{X\in\mathcal{B}} X$ and $\bigcap_{X\in\mathcal{B}} X$
6. Use the roster method to specify the sets $(\bigcup_{X\in\mathcal{A}} X)^c$ and $\bigcap_{X\in\mathcal{A}} X^c$. Remember that the universal set is $\mathbb{N}$.

? Preview Activity 5.5.2: An Indexed Family of Sets

We often use subscripts to identify sets. For example, in Preview Activity 5.5.1, instead of using A, B, C, and D as the names of the sets, we could have used A_1, A_2, A_3, and A_4. When we do this, we are using the subscript as an identifying tag, or index, for each set. We can also use this idea to specify an infinite family of sets. For example, for each natural number n, we define

$$C_n = \{n, n+1, n+2, n+3, n+4\}.$$

So if we have a family of sets $\mathcal{C} = \{C_1, C_2, C_3, C_4\}$, we use the notation $\bigcup_{j=1}^{4} C_j$ to mean the same thing as $\bigcup_{x\in\mathcal{C}} X$.

1. Determine $\bigcup_{j=1}^{4} C_j$ and $\bigcap_{j=1}^{4} C_j$

   We can see that with the use of subscripts, we do not even have to define the family of sets $\mathcal{A}$. We can work with the infinite family of sets

$$\mathcal{C}^* = \{A_n \mid n \in \mathbb{N}\} \tag{5.5.1}$$

   and use the subscripts to indicate which sets to use in a union or an intersection.
2. Use the roster method to specify each of the following pairs of sets. The universal set is $\mathbb{N}$.

   (a) $\bigcup_{j=1}^{6} C_j$ and $\bigcap_{j=1}^{6} C_j$
   (b) $\bigcup_{j=1}^{8} C_j$ and $\bigcap_{j=1}^{8} C_j$
   (c) $\bigcup_{j=4}^{8} C_j$ and $\bigcap_{j=4}^{8} C_j$
   (d) $(\bigcap_{j=1}^{4} C_j)^c$ and $\bigcup_{j=1}^{4} C_j^c$

The Union and Intersection over an Indexed Family of Sets

One of the purposes of the preview activities was to show that we often encounter situations in which more than two sets are involved, and it is possible to define the union and intersection of more than two sets. In Preview Activity 5.5.2, we also saw that it is often convenient to "index" the sets in a family of sets. In particular, if n is a natural number and $\mathcal{A} = \{A_1, A_2, \ldots, A_n\}$ is a family of n sets, then the union of these n sets, denoted by $A_1 \cup A_2 \cup \cdots \cup A_n$ or $\bigcup_{j=1}^{n} A_j$, is defined as

$$\bigcup_{j=1}^{n} A_j = \{x \in U \mid x \in A_j, \text{ for some } j \text{ with } 1 \le j \le n\}. \tag{5.5.2}$$

We can also defined the intersection of these n sets, denoted by $A_1 \cap A_2 \cap \cdots \cap A_n$ or $\bigcap_{j=1}^{n} A_j$, as

$$\bigcap_{j=1}^{n} A_j = \{x \in U \mid x \in A_j, \text{ for some } j \text{ with } 1 \le j \le n\}. \tag{5.5.3}$$

We can also extend this idea to define the union and intersection of a family that consists of infinitely many sets. So if $\mathcal{B} = \{B_1, B_2, \ldots, B_n, \ldots\}$, then

$\bigcup_{j=1}^{\infty} B_j = \{x \in U \mid x \in B_j, \text{ for some } j \text{ with } j \ge 1\}$, and

$\bigcap_{j=1}^{\infty} B_j = \{x \in U \mid x \in B_j, \text{ for all } j \text{ with } j \ge 1\}$.

? Progress Check 5.26 (An Infinite Family of Sets)

For each natural number n, let $A_n = \{1, n, n^2\}$. For example,

$A_1 = \{1\}$, $A_2 = \{1, 2, 4\}$, $A_3 = \{1, 3, 9\}$, and

$\bigcup_{j=1}^{3} A_j = \{1, 2, 3, 4, 9\}$, $\bigcap_{j=1}^{3} A_j = \{1\}$.

Determine each of the following sets:

1. $\bigcup_{j=1}^{6} A_j$
2. $\bigcap_{j=1}^{6} A_j$
3. $\bigcup_{j=3}^{6} A_j$
4. $\bigcap_{j=3}^{6} A_j$
5. $\bigcup_{j=1}^{\infty} A_j$
6. $\bigcap_{j=1}^{\infty} A_j$

Answer

Add texts here. Do not delete this text first.

In all of the examples we have studied so far, we have used $\mathbb{N}$ or a subset of $\mathbb{N}$ to index or label the sets in a family of sets. We can use other sets to index or label sets in a family of sets. For example, for each real number x, we can define B_x to be the closed interval [x, x + 2]. That is,

$$B_x = \{y \in \mathbb{R} \mid x \le y \le x + 2\}.$$

So we make the following definition. In this definition,$\wedge$ is the uppercase Greek letter lambda and α is the lowercase Greek letter alpha.

Definition

Let Λ be a nonempty set and suppose that for each $\alpha \in \wedge$, there is a corresponding set A_α. The family of sets $\{A_\alpha \mid \alpha \in \wedge\}$ is called an **indexed family of sets** indexed by $\wedge$. Each $\alpha \in \wedge$ is called an **index** and Λ is called an **indexing set**.

Progress Check 5.27 (Indexed Families of Sets)

In each of the indexed families of sets that we seen so far, if the indices were different, then the sets were different. That is, if Λ is an indexing for the family of sets $\mathcal{A} = \{A_\alpha \mid \alpha \in \wedge\}$, then if $\alpha, \beta \in \wedge$ and $\alpha \ne \beta$, then $A_\alpha \ne A_\beta$. (**Note**: The letter β is the Greek lowercase beta.)

1. Let $\Lambda = \{1, 2, 3, 4\}$, and for each $n \in \Lambda$, let $A_n = \{2n + 6, 16 - 3n\}$, and let $\mathcal{A} = \{A_1, A_2, A_3, A_4\}$. Determine A_1, A_2, A_3, and A_4.
2. Is the following statement true or false for the indexed family $\mathcal{A}$ in (1)?
3. Now let $\Lambda = \mathbb{R}$. For each $x \in \mathbb{R}$, define $B_x = \{0, x^2, x^4\}$. Is the following statement true for the indexed family of set $\mathcal{B} = \{B_x \mid x \in \mathbb{R}\}$?
   For all $x, y \in \mathbb{R}$, if $x \ne y$, then $B_x \ne B_y$.

Answer

Add texts here. Do not delete this text first.

We now restate the definitions of the union and intersection of a family of sets for an indexed family of sets.

Definition

Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets. The union over $\mathcal{A}$ is defined as the set of all elements that are in at least one of sets A_α, where $\alpha \in \wedge$. We write

$$\bigcup_{\alpha \in \Lambda} A_\alpha = \{x \in U \mid \text{ there exits an } \alpha \in \Lambda \text{ with } x \in A_\alpha\}.$$

The intersection over (\mathcal{A}\) is the set of all elements that are in all of the sets A_α for each $\alpha \in \Lambda$. That is,

$$\bigcap_{\alpha \in \wedge} A_\alpha = \{x \in U \mid \text{ for all } \alpha \in \wedge, x \in A_\alpha\}.$$

Example 5.28 (A Family of Sets Indexed by the Positive Real Numbers)

For each positive real numbe α, let A_α be the interval (-1, α]. That is,

$$A_\alpha = \{x \in \mathbb{R} \mid -1 < x \leq \alpha\}.$$

If we let $\mathbb{R}^+$ be the set of positive real numbers, then we have a family of sets indexed by $\mathbb{R}^+$. We will first determine the union of this family of sets. Notice that for each $\alpha \in mathbbR^+$, $\alpha \in A_\alpha$, and if y is a real number with $-1 < y \leq 0$, then $y \in A_\alpha$. Also notice that if $y \in \mathbb{R}$ and $y < -1$, then for each $\alpha \in mathbbR^+$, $y \notin A_\alpha$. With these observations, we conclude that

$$\bigcup_{\alpha \in \mathbb{R}^+} A_\alpha = (-1, \infty) = \{x \in \mathbb{R} \mid -1 < x\}.$$

To determine the intersection of this family, notice that

- if $y \in \mathbb{R}$ and $y < -1$, then for each $\alpha \in \mathbb{R}^+$, $y \notin A_\alpha$;
- if $y \in \mathbb{R}$ and $-1 < y \leq 0$, then $y \in A_\alpha$ for each $\alpha \in mathbbR^+$; and
- if $y \in \mathbb{R}$ and $y > 0$, then of we let $\beta = \dfrac{y}{2}$, $y > \beta$ and $y \notin A_\beta$.

From these observations, we conclude that

$$\bigcap_{\alpha \in \mathbb{R}^+} A_\alpha = (-1, 0] = \{x \in \mathbb{R} \mid -1 < x \leq 0\}.$$

Progress Check 5.29 (A Continuation of Example 5.28)

Using the family of sets from Example 5.28, for each $\alpha \in mathbbR^+$, we see that

$A^c_\alpha = (-\infty, 1] \cup (\alpha, \infty)$.

Use the results from Example 5.28 to help determine each of the following sets. For each set, use either interval notation or set builder notation.

1. $\left(\bigcup_{\alpha \in \mathbb{R}^+} A_\alpha\right)^c$
2. $\left(\bigcap_{\alpha \in \mathbb{R}^+} A_\alpha\right)^c$
3. $\bigcap_{\alpha \in \mathbb{R}^+} A^c_\alpha$
4. $\bigcup_{\alpha \in \mathbb{R}^+} A^c_\alpha$

Answer

Add texts here. Do not delete this text first.

Properties of Union and Intersection

In Theorem 5.30, we will prove some properties of set operations for indexed families of sets. Some of these properties are direct extensions of corresponding properties for two sets. For example, we have already proved De Morgan's Laws for two sets in Theorem 5.20. The work in the preview activities and Progress Check 5.29 suggests that we should get similar results using set operations with an indexed family of sets. For example, in Preview Activity $5.5.2$, we saw that

$$\left(\bigcap_{j=1}^{4} A_j\right)^c = \bigcup_{j=1}^{4} A^c_j.$$

Theorem 5.30.

Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \wedge\}$ be an indexed family of sets. Then

1. For each $\beta \in \Lambda$, $\bigcap_{\alpha \in \Lambda} A_\alpha \subseteq A_\beta$
2. For each $\beta \in \Lambda$, $A_\beta \subseteq \bigcup_{\alpha \in \Lambda} A_\alpha$
3. $\left(\bigcap_{\alpha \in \Lambda} A_\alpha\right)^c = \bigcup_{\alpha \in \Lambda} A^c_\alpha$
4. $\left(\bigcup_{\alpha \in \Lambda} A_\alpha\right)^c = \bigcap_{\alpha \in \Lambda} A^c_\alpha$

Parts (3) and (4) are known as ***De Morgan's Laws.***

Proof

We will prove Parts (1) and (3). The proofs of Parts (2) and (4) are included in Exercise (4). So we let Λ be a nonempty indexing set and let $mathcalA = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets. To prove Part (1), we let $\beta \in \Lambda$ and note that if $x \in \bigcap_{\alpha \in \Lambda} A_\alpha$, then $x \in A_\alpha$, for all $\alpha \in \Lambda$. Since β is one element in Λ, we may conclude that $x \in A_\beta$. This proves that $\bigcap_{\alpha \in \Lambda} A_\alpha \subseteq A_\beta$.

To prove Part (3), we will prove that each set is a subset of the other set. We first let $x \in (\bigcap_{\alpha \in \Lambda} A_\alpha)^c$. This means that $x \notin (\bigcap_{\alpha \in \Lambda} A_\alpha)$, and this means that

$$\text{there exists a } \beta \in \Lambda \text{ such that } x \notin A_\beta.$$

Hence, $x \in A_\beta^c$, which implies that $x \in \bigcup_{\alpha \in \Lambda} A_\alpha^c$. Therefore, we have proved that

$$(\bigcap_{\alpha \in \Lambda} A_\alpha)^c \subseteq \bigcup_{\alpha \in \Lambda} A_\alpha^c. \tag{5.5.4}$$

We now let $y \in \bigcup_{\alpha \in \Lambda} A_\alpha^c$. This means that there exists a $\beta \in \Lambda$ such that $y \in A_\beta^c$ or $y \notin A_\beta$. However, since $y \notin A_\beta$, we may conclude that $y \notin \bigcap_{\alpha \in \Lambda} A_\alpha$ and, hence, $y \in (\bigcap_{\alpha \in \Lambda} A_\alpha)^c$. This proves that

$$\bigcup_{\alpha \in \Lambda} A_\alpha^c \subseteq (\bigcap_{\alpha \in \Lambda} A_\alpha)^c. \tag{5.5.5}$$

Using the results in (5.5.4) and (5.5.5), we have proved that $(\bigcap_{\alpha \in \Lambda} A_\alpha)^c = \bigcup_{\alpha \in \Lambda} A_\alpha^c$.

Many of the other properties of set operations are also true for indexed families of sets. Theorem 5.31 states the distributive laws for set operations.

Theorem 5.31.

Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets, and let B be a set. Then

1. $B \cap (\bigcup_{\alpha \in \Lambda} A_\alpha) = \bigcup_{\alpha \in \Lambda} (B \cap A_\alpha)$, and
2. $B \cup (\bigcap_{\alpha \in \Lambda} A_\alpha) = \bigcap_{\alpha \in \Lambda} (B \cup A_\alpha)$.

Proof

The proof of Theorem 5.31 is Exercise (5).

Pairwise Disjoint Families of Sets

In Section 5.2, we defined two sets A and B to be disjoint provided that $A \cap B = \emptyset$. In a similar manner, if Λ is a nonempty indexing set and $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ is an indexed family of sets, we can say that this indexed family of sets is **disjoint** provided that $\bigcap_{\alpha \in \Lambda} A_\alpha = \emptyset$. However, we can use the concept of two disjoint sets to define a somewhat more interesting type of "disjointness" for an indexed family of sets.

Definition

Let Λ be a nonempty indexing set, and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets. We say that $\mathcal{A}$ is pair wise disjoint provided that for all α and β in Λ, if $A_\alpha \neq A_\beta$, then $A_\alpha \cap A_\beta = \emptyset$.

Progress Check 5.32 (Disjoint Families of Sets)

Figure 5.7 shows two families of sets,

$$\mathcal{A} = \{A_1, A_2, A_3, A_4\} \text{ and } \mathcal{B} = \{B_1, B_2, B_3, B_4\}.$$

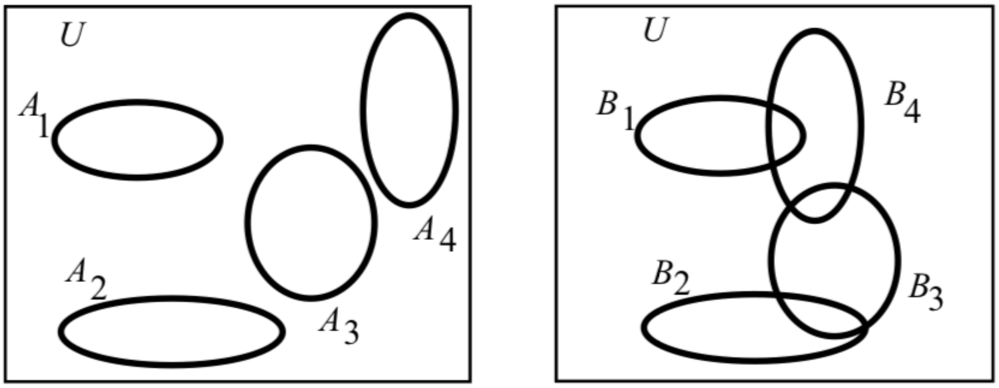


Figure 5.7: Two Families of Indexed Sets

1. Is the family of sets $\mathcal{A}$ a disjoint family of sets? A pairwise disjoint family of sets?
2. Is the family of sets $\mathcal{B}$ a disjoint family of sets? A pairwise disjoint family of sets?

   Now let the universal be $\mathbb{R}$. For each $n \in \mathbb{N}$, let $C_n = (n, \infty)$, and let $\mathcal{C} = \{C_n \mid n \in \mathbb{N}\}$.
3. Is the family of sets $\mathcal{C}$ a disjoint family of sets? A pairwise disjoint family of sets?

Answer

Add texts here. Do not delete this text first.

Exercise 5.5.1

1. For each natural number n, let $A_n = \{n, n+1, n+2, n+3\}$. Use the roster method to specify each of the following sets:

   (a) $\bigcap_{j=1}^{3} A_j$
   (b) $\bigcup_{j=1}^{3} A_j$
   (c) $\bigcap_{j=3}^{7} A_j$
   (d) $\bigcup_{j=3}^{7} A_j$
   (e) $A_9 \cap (\bigcup_{j=3}^{7} A_j)$
   (f) $\bigcup_{j=3}^{7} (A_9 \cap A_j)$
2. For each natural number n, let $A_n = \{k \in \mathbb{N} \mid k \geq n\}$. Use the roster method or set builder notation to specify each of the following sets:

   (a) $\bigcap_{j=1}^{5} A_j$
   (b) $(\bigcap_{j=1}^{5} A_j)^c$
   (c) $\bigcap_{j=1}^{5} A_j^c$
   (d) $\bigcup_{j=1}^{5} A_j^c$
   (e) $\bigcup_{j=1}^{5} A_j$
   (f) $(\bigcup_{j=1}^{5} A_j)^c$
   (g) \(\bigcap_{j \in \mathbb{N}^{} A_j\)
   (h) \(\bigcup_{j \in \mathbb{N}^{} A_j\)
3. For each positive real number r, define T_r to be the closed interval $[-r^2, r^2]$. That is

$$T_r = \{x \in \mathbb{R} \mid -r^2 \leq x \leq r^2\}. \tag{5.5.6}$$

Let $\wedge = \{m \in \mathbb{N} \mid 1 \le m \le 10\}$. Use either interval notation or set builder notation to specify each of the following sets:

(a) $\bigcup_{k \in \wedge} T_k$
(b) $\bigcap_{k \in \wedge} T_k$
(c) $\bigcup_{r \in \mathbb{R}^+} T_k$
(d) $\bigcap_{r \in \mathbb{R}^+} T_k$
(e) $\bigcup_{r \in \mathbb{N}} T_k$
(f) $\bigcap_{r \in \mathbb{N}} T_k$

4. Prove Parts (2) and (4) of Theorem 5.30. Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets.

   (a) For each $\beta \in \Lambda$, $A_\beta \subseteq \bigcup_{\alpha \in \Lambda} A_\alpha$.
   (b) $(\bigcup_{\alpha \in \Lambda} A_\alpha)^c = \bigcap_{\alpha \in \Lambda} A_\alpha^c$
5. Prove Theorem 5.31. Let Λ be a nonempty indexing set, let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets, and let B be a set. Then

   (a) $B \cap (\bigcup_{\alpha \in \Lambda} A_\alpha) = \bigcup_{\alpha \in \Lambda}(B \cap A_\alpha)$, and
   (b) $B \cup (\bigcap_{\alpha \in \Lambda} A_\alpha) = \bigcap_{\alpha \in \Lambda}(B \cup A_\alpha)$.
6. Let Λ and Γ be nonempty indexing sets and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ and $\mathcal{B} = \{B_\beta \mid \beta \in \Gamma\}$ be indexed families of sets. Use the distributive laws in Exercise (5) to:

   (a) Write \((\bigcup_{\alpha \in \Lambda}^{} A_{\alpha}) \cap (\bigcup_{\beta \in \Gamma}^{} B_{\beta}) as a union of intersections of two sets.
   (b) Write \((\bigcap_{\alpha \in \Lambda}^{} A_{\alpha}) \cup (\bigcap_{\beta \in \Gamma}^{} B_{\beta}) as a union of intersections of two sets.
7. Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets. Also, assume that $\Gamma \subseteq \Lambda$ and $\Gamma \ne \emptyset$. (**Note**: The letter Γ is the uppercase Greek letter gamma.) Prove that

   (a) $\bigcup_{\alpha \in \Gamma} A_\alpha \subseteq \bigcup_{\alpha \in \Lambda} A_\alpha$
   (b) $\bigcap_{\alpha \in \Lambda} A_\alpha \subseteq \bigcap_{\alpha \in \Gamma} A_\alpha$
8. Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets.

   (a) Prove that if B is a set such that $B \subseteq A_\alpha$ for every $\alpha \in \Lambda$, then $B \subseteq \bigcap_{\alpha \in \Lambda} A_\alpha$.
   (b) Prove that if C is a set such that $A_\alpha \subseteq C$ for every $\alpha \in \Lambda$, then $\bigcap_{\alpha \in \Lambda} A_\alpha \subseteq C$.
9. For each natural number n, let $A_n = \{x \in \mathbb{R} \mid n - 1 < x < n\}$. Prove that $\{A_n \mid n \in \mathbb{N}\}$ is a pairwise disjoint family of sets and that $\bigcup_{n \in \mathbb{N}} A_n = (\mathbb{R}^+ - \mathbb{N})$.
10. For each natural number n, let $A_n = \{k \in \mathbb{N} \mid k \ge n\}$. Determine if the following statements are true or false. Justify each conclusion.

    (a) For all $j, k \in \mathbb{N}$, if $j \ne k$, then $A_j \cap A_k \ne \emptyset$.
    (b) $\bigcap_{k \in \mathbb{N}} A_k = \emptyset$.
11. Give an example of an indexed family of sets $\{A_n \mid n \in \mathbb{N}\}$ such all three of the following conditions are true:

    (i) For each $m \in \mathbb{N}$, $A_m \subseteq (0, 1)$;
    (ii) For each $j, k \in \mathbb{N}$, if $j \ne k$, then $A_j \cap A_k \ne \emptyset$; and
    (iii) $\bigcap_{k \in \mathbb{N}} A_k = \emptyset$.
12. Let Λ be a nonempty indexing set, let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets, and let B be a set. Use the results of Theorem 5.30 and Theorem 5.31 to prove each of the following:

    (a) $(\bigcup_{\alpha \in \Lambda} A_\alpha) - B = \bigcup_{\alpha \in \Lambda}(A_\alpha - B)$
    (b) $(\bigcap_{\alpha \in \Lambda} A_\alpha) - B = \bigcap_{\alpha \in \Lambda}(A_\alpha - B)$

(c) $B-(\bigcup_{\alpha\in\Lambda}A_\alpha)=\bigcap_{\alpha\in\Lambda}B-(A_\alpha)$
(d) $B-(\bigcap_{\alpha\in\Lambda}A_\alpha)=\bigcup_{\alpha\in\Lambda}B-(A_\alpha)$

Explorations and Activities

13. An Indexed Family of Subsets of the Cartesian Plane. Let $\mathbb{R}^*$ be the set of nonnegative real numbers, and for each $r\in\mathbb{R}^*$, let

$$\begin{aligned} C_r &= \{(x,y)\in\mathbb{R}\times\mathbb{R} \mid x^2+y^2=r^2\} \\ D_r &= \{(x,y)\in\mathbb{R}\times\mathbb{R} \mid x^2+y^2\le r^2\} \\ T_r &= \{(x,y)\in\mathbb{R}\times\mathbb{R} \mid x^2+y^2>r^2\}=D_r^c. \end{aligned} \tag{5.5.7}$$

If $r>0$, then the set C_r is the circle of radius r with center at the origin as shown in Figure 5.8, and the set D_r is the shaded disk (including the boundary) shown in Figure 5.8.

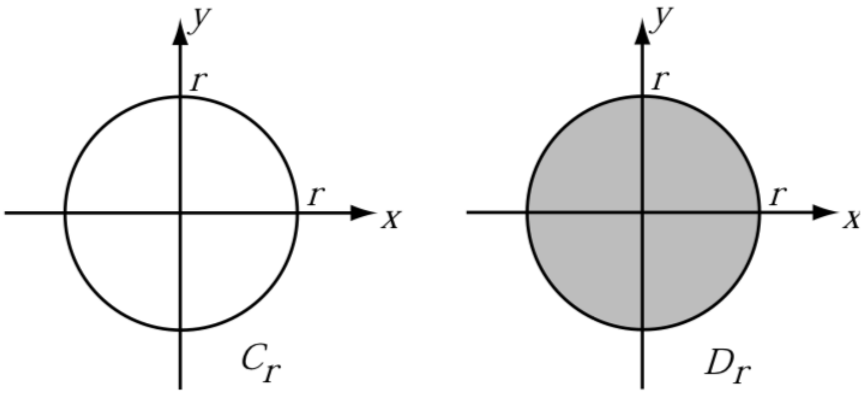


Figure 5.8: Two Sets for Activity 13

(a) Determine $\bigcup_{r\in\mathbb{R}^*}C_r$ and $\bigcap_{r\in\mathbb{R}^*}C_r$
(b) Determine $\bigcup_{r\in\mathbb{R}^*}D_r$ and $\bigcap_{r\in\mathbb{R}^*}D_r$
(c) Determine $\bigcup_{r\in\mathbb{R}^*}T_r$ and $\bigcap_{r\in\mathbb{R}^*}T_r$
(d) Let $\mathcal{C}=\{C_r \mid r\in\mathbb{R}^*\}$, $\mathcal{D}=\{D_r \mid r\in\mathbb{R}^*\}$, and $\mathcal{T}=\{T_r \mid r\in\mathbb{R}^*\}$. Are any of these indexed families of sets pairwise disjoint? Explain.

Now let I be the closed interval [0, 2] and let J be the closed interval [1, 2].
(e) Determine $\bigcup_{r\in I}C_r$, $\bigcap_{r\in I}C_r$, $\bigcup_{r\in J}C_r$, and $\bigcap_{r\in J}C_r$
(f) Determine $\bigcup_{r\in I}D_r$, $\bigcap_{r\in I}D_r$, $\bigcup_{r\in J}D_r$, and $\bigcap_{r\in J}D_r$
(g) Determine $(\bigcup_{r\in I}D_r)^c$, $(\bigcap_{r\in I}D_r)^c$, $(\bigcup_{r\in J}D_r)^c$, and $(bigcap_{r\in J}D_r)^c$
(h) Determine $\bigcup_{r\in I}T_r$, $\bigcap_{r\in I}T_r$, $\bigcup_{r\in J}T_r$, and $\bigcap_{r\in J}T_r$
(i) Use De Morgan's Laws to explain the relationship between your answers in Parts (13g) and (13h).

Answer

Add texts here. Do not delete this text first.

This page titled 5.5: Indexed Families of Sets is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

5.S: Set Theory (Summary)

Important Definitions

- Equal sets, page 55
- Subset, page 55
- Proper subset, page 218
- Power set, page 222
- Cardinality of a finite set, page 223
- Intersection of two sets, page 216
- Union of two sets, page 216
- Set difference, page 216
- Complement of a set, page 216
- Disjoint sets, page 236
- Cartesian product of two sets, pages 256
- Ordered pair, page 256
- Union over a family of sets, page 265
- Intersection over a family of sets, page 265
- Indexing set, page 268
- Indexed family of sets, page 268
- Union over an indexed family of sets, page 269
- Intersection over an indexed family of sets, page 269
- Pairwise disjoint family of sets, page 272

Important Theorems and Results about Sets

- **Theorem 5.5**. Let n be a nonnegative integer and let A be a subset of some universal set. If A is a finite set with n elements, then A has 2^n subsets. That is, if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.
- **Theorem 5.18**. Let A, B, and C be subsets of some universal set U. Then all of the following equalities hold.

  Properties of the Empty Set $A \cap \emptyset = \emptyset$ $A \cap U = A$
  and the Universal Set $A \cup \emptyset = A$ $A \cup U = U$

  Idempotent Laws $A \cap A = A$ $A \cup A = A$

  Commutative Laws. $A \cap B = B \cap A$ $A \cup B = B \cup A$

  Associative Laws $(A \cap B) \cap C = A \cap (B \cap C)$
  $(A \cup B) \cup C = A \cup (B \cup C)$

  Distributive Laws $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- **Theorem 5.20**. Let A and B be subsets of some universal set U. Then the following are true:

$$\begin{array}{ll}
\text{Basic Properties} & (A^c)^c = A \\
 & A - B = A \cap B^c \\
\text{Empty Set, Universal Set} & A - \emptyset = A \text{ and } A - U = \emptyset \\
 & \emptyset^c = U \text{ and } U^c = \emptyset \\
\text{De Morgan's Laws} & (A \cap B)^c = A^c \cup B^c \\
 & (A \cup B)^c = A^c \cap B^c \\
\text{Subsets and Complements} & A \subseteq B \text{ if and only if } B^c \subseteq A^c.
\end{array} \tag{5.S.1}$$

- **Theorem 5.25**. Let A, B, and C be sets. Then

  1. $A \times (B \cap C) = (A \times B) \cap (A \times C)$

    2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
    3. $(A \cap B) \times C = (A \times C) \cap (B \times C)$
    4. $(A \cup B) \times C = (A \times C) \cup (B \times C)$
    5. $A \times (B - C) = (A \times B) - (A \times C)$
    6. $(A - B) \times C = (A \times C) - (B \times C)$
    7. If $T \subseteq A$, then $T \times B \subseteq A \times B$.
    8. If $T \subseteq B$, then $A \times Y \subseteq A \times B$.
- **Theorem 5.30**. Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets. Then

    1. For each $\beta \in \Lambda$, $\bigcap_{\alpha \in \Lambda} A_\alpha \subseteq A_\beta$.
    2. For each $\beta \in \Lambda$, $A_\beta \subseteq \bigcap_{\alpha \in \Lambda} A_\alpha$.
    3. $(\bigcap_{\alpha \in \Lambda} A_\alpha)^c = \bigcup_{\alpha \in \Lambda} A_\alpha^c$
    4. $(\bigcup_{\alpha \in \Lambda} A_\alpha)^c = \bigcap_{\alpha \in \Lambda} A_\alpha^c$

    Parts(3) and (4) are known as ***De Morgan's Laws***.
- **Theorem 5.31**. Let Λ be a nonempty indexing set, let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets, and let B be a set. Then

    1. $B \cap (\bigcup_{\alpha \in \Lambda} A_\alpha) = \bigcup_{\alpha \in \Lambda} (B \cap A_\alpha)$, and
    2. $B \cup (\bigcap_{\alpha \in \Lambda} A_\alpha) = \bigcap_{\alpha \in \Lambda} (B \cup A_\alpha)$,

Important Proof Method

The Choose-an-Element Method

The choose-an-element method is frequently used when we encounter a universal quantifier in a statement in the backward process of a proof. This statement often has the form

For each element with a given property, something happens.

In the forward process of the proof, we then we choose an arbitrary element with the given property.

> Whenever we choose an arbitrary element with a given property, we are not selecting a specific element. Rather, the only thing we can assume about the element is the given property.

For more information, see page 232.

page297image2085397184page297image2085397456

This page titled 5.S: Set Theory (Summary) is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

CHAPTER OVERVIEW

6: Functions

6.1: Introduction to Functions
6.2: More about Functions
6.3: Injections, Surjections, and Bijections
6.4: Composition of Functions
6.5: Inverse Functions
6.6: Functions Acting on Sets
6.S: Functions (Summary)

This page titled 6: Functions is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

6.1: Introduction to Functions

Exercise 6.1.1

Preview Activity 1 (Functions from Previous Courses)

One of the most important concepts in modern mathematics is that of a **function**. In previous mathematics courses, we have often thought of a function as some sort of input-output rule that assigns exactly one output to each input. So in this context, a **function** can be thought of as a procedure for associating with each element of some set, called the **domain of the function**, exactly one element of another set, called the **codomain of the function**. This procedure can be considered an input-output-rule. The function takes the input, which is an element of the domain, and produces an output, which is an element of the codomain. In calculus and precalculus, the inputs and outputs were almost always real numbers. So the notationf $f(x) = x^2 sinx$ means the following:

- f is the name of the function.
- $f(x)$ is a real number. It is the output of the function when the input is the real number x. For example,

$$\begin{aligned} f(\frac{\pi}{2}) &= (\frac{\pi}{2})^2 sin(\frac{\pi}{2}) \\ &= \frac{\pi^2}{4} \cdot 1 \\ &= \frac{\pi^2}{4}. \end{aligned} \tag{6.1.1}$$

For this function, it is understood that the domain of the function is the set $\mathbb{R}$ of all real numbers. In this situation, we think of the domain as the set of all possible inputs. That is, the domain is the set of all possible real numbers x for which a real number output can be determined.

This is closely related to the equation $f = x^2 sinx$. With this equation, we frequently think of x as the input and y as the output. In fact, we sometimes write $y = f(x)$. The key to remember is that a function must have exactly one output for each input. When we write an equation such as

$$y = \frac{1}{2}x^3 - 1,$$

we can use this equation to define y as a function of x. This is because when we substitute a real number for x (the input), the equation produces exactly one real number for y (the output). We can give this function a name, such as g, and write

$$y = g(x) = \frac{1}{2}x^3 - 1.$$

However, as written, an equation such as

$$y^2 = x + 3$$

cannot be used to define y as a function of x since there are real numbers that can be substituted for x that will produce more than one possible value of y. For example, if $x = 1$, then $y^2 = 4$, and y could be -2 or 2.

Which of the following equations can be used to define a function with $x \in \mathbb{R}$ as the input and $y \in \mathbb{R}$ as the output?

1. $y = x^2 - 2$
2. $y^2 = x + 3$
3. $y = \frac{1}{2}x^3 - 1$
4. $y = \frac{1}{2}x sinx$
5. $x^2 + y^2 = 4$
6. $y = 2x - 1$
7. $y = dfracxx - 1$

✓ Preview Activity 2 (Some Other Types of Functions)

The domain and codomain of the functions in Preview Activity $6.1.1$ is the set $\mathbb{R}$ of all real numbers, or some subset of $\mathbb{R}$. In most of these cases, the way in which the function associates elements of the domain with elements of the codomain is by a rule determined by some mathematical expression. For example, when we say that f is the function such that

$$f(x) = \frac{x}{x-1},$$

then the algebraic rule that determines the output of the function f when the input is x is $\frac{x}{x-1}$. In this case, we would say that the domain of f is the set of all real numbers not equal to 1 since division by zero is not defined.

However, the concept of a function is much more general than this. The domain and codomain of a function can be any set, and the way in which a function associates elements of the domain with elements of the codomain can have many different forms. The input-output rule for a function can be a formula, a graph, a table, a random process, or a verbal description. We will explore two different examples in this preview activity.

1. Let b be the function that assigns to each person his or her birthday (month and day). The domain of the function b is the set of all people and the codomain of b is the set of all days in a leap year (i.e., January 1 through December 31, including February 29).

   (a) Explain why b really is a function. We will call this the **birthday function**.
   (b) In 1995, Andrew Wiles became famous for publishing a proof of Fermat's Last Theorem. (See A. D. Aczel, *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem,* Dell Publishing, New York, 1996.) Andrew Wiles's birthday is April 11, 1953. Translate this fact into functional notation using the "birthday function" b. That is, fill in the spaces for the following question marks:

   $$b(?) = ?. \tag{6.1.2}$$

   (c) Is the following statement true or false? Explain.
   For each day D of the year, there exists a person x such that $b(x) = D$.
   (d) Is the following statement true or false? Explain.
   For any people x and y, if x and y are different people, then $b(x) \neq b(y)$.
2. Let s be the function that associates with each natural number the sum of its distinct natural number divisors. This is called the **sum of the divisors function**. For example, the natural number divisors of 6 are 1, 2, 3, and 6, and so

   $$\begin{aligned} s(6) &= 1+2+3+6 \\ &= 12. \end{aligned} \tag{6.1.3}$$

   (a) Calculate $s(k)$ for each natural number k from 1 through 15.
   (b) Does there exist a natural number n such that $s(n) = 5$? Justify your conclusion.
   (c) Is it possible to find two different natural numbers m and n such that $s(m) = s(n)$? Explain.
   (d) Use your responses in (b) and (c) to determine whether the following statements true or false.
   i. For each $m \in \mathbb{N}$, there exists a natural number n such that $s(n) = m$.
   ii. For all $m, n \in \mathbb{N}$, if $m \neq n$, then $s(m) \neq s(n)$.

The Definition of a Function

The concept of a function is much more general than the idea of a function used in calculus or precalculus. In particular, the domain and codomain do not have to be subsets of $\mathbb{R}$. In addition, the way in which a function associates elements of the domain with elements of the codomain can have many different forms. This input-output rule can be a formula, a graph, a table, a random process, a computer algorithm, or a verbal description. Two such examples were introduced in Preview Activity $6.1.2$.

For the **birthday function**, the domain would be the set of all people and the codomain would be the set of all days in a leap year. For the **sum of the divisors function**, the domain is the set $\mathbb{N}$ of natural numbers, and the codomain could also be $\mathbb{N}$. In both of these cases, the input-output rule was a verbal description of how to assign an element of the codomain to an element of the domain.

We formally define the concept of a function as follows:

Definition

A *function* from a set A to a set B is a rule that associates with each element x of the set A exactly one element of the set B. A function from A to B is also called a *mapping* from A to B.

Function Notation. When we work with a function, we usually give it a name. The name is often a single letter, such as f or g. If f is a function from the set A to be the set B, we will write $f : A \to B$. This is simply shorthand notation for the fact that f is a function from the set A to the set B. In this case, we also say that f maps A to B.

Definition

Let $f : A \to B$. (This is read, "Let f be a function from A to B.") The set A is called the **domain** of the function f, and we write $A = dom(f)$. The set B is called the **codomain** of the function f, and we write $B = codom(f)$.

If $a \in A$, then the element of B that is associated with a is denoted by $f(a)$ and is called the ***image of a under*** f. If $f(a) = b$, with $b \in B$, then a is called a **preimage of** b **under** f.

Some Function Terminology with an Example. When we have a function $f : A \to B$, we often write $y = f(x)$. In this case, we consider x to be an unspecified object that can be chosen from the set A, and we would say that x is the **independent variable** of the function f and y is the **dependent variable** of the function f.

For a specific example, consider the function $g : \mathbb{R} \to \mathbb{R}$, where $g(x)$ is defined by the formula

$$g(x) = x^2 - 2.$$

Note that this is indeed a function since given any input x in the domain, $\mathbb{R}$, there is exactly one output $g(x)$ in the codomain, $\mathbb{R}$. For example,

$$\begin{aligned} g(-2) &= (-2)^2 - 2 = 2, \\ g(5) &= 5^2 - 2 = 23, \\ g(\sqrt{2}) &= (\sqrt{2})^2 - 2 = 0, \\ g(-\sqrt{2}) &= (-\sqrt{2})^2 - 2 = 0. \end{aligned} \tag{6.1.4}$$

So we say that the image of -2 under g is 2, the image of 5 under g is 23, and so on.

Notice in this case that the number 0 in the codomain has two preimages, $-\sqrt{2}$ and $\sqrt{2}$. This does not violate the mathematical definition of a function since the definition only states that each input must produce one and only one output. That is, each element of the domain has exactly one image in the codomain. Nowhere does the definition stipulate that two different inputs must produce different outputs.

Finding the preimages of an element in the codomain can sometimes be difficult. In general, if y is in the codomain, to find its preimages, we need to ask, "For which values of x in the domain will we have $y = g(x)$?" For example, for the function g, to find the preimages of 5, we need to find all x for which $g(x) = 5$. In this case, since $g(x) = x^2 - 2$, we can do this by solving the equation

$$x^2 - 2 = 5.$$

The solutions of this equation are $-\sqrt{7}$ and $\sqrt{7}$. So for the function g, the preimages of 5 are $-\sqrt{7}$ and $\sqrt{7}$. We often use set notation for this and say that the set of preimages of 5 for the function g is $\{-\sqrt{7}, \sqrt{7}\}$.

Also notice that for this function, not every element in the codomain has a preimage. For example, there is no input x such that $g(x) = -3$. This is true since for all real numbers x, $x^2 \geq 0$ and hence $x^2 - 2 \geq -2$. This means that for all x in $\mathbb{R}$, $g(x) \geq -2$.

Finally, note that we introduced the function g with the sentence, "Consider the function $g : \mathbb{R} \to \mathbb{R}$, where $g(x)$ is defined by the formula $g(x) = x^2 - 2$." This is one correct way to do this, but we will frequently shorten this to, "Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^2 - 2$", or "Let $g : \mathbb{R} \to \mathbb{R}$, where $g(x) = x^2 - 2$."

Progress Check 6.1 (Images and Preimages)

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 - 5x$ for all $x \in \mathbb{R}$. and let $g : \mathbb{Z} \to \mathbb{Z}$ be defined by $g(m) = m^2 - 5m$ for all $m \in \mathbb{Z}$.

1. Determine $f(-3)$ and $f(\sqrt{8})$.
2. Determine $g(2)$ and $g(-2)$.
3. Determine the set of all preimage of 6 for the function f.
4. Determine the set of all preimage of 6 for the function g.
5. Determine the set of all preimage of 2 for the function f.
6. Determine the set of all preimage of 2 for the function g.

Answer

Add texts here. Do not delete this text first.

The Codomain and Range of a Function

Besides the domain and codomain, there is another important set associated with a function. The need for this was illustrated in the example of the function g on page 285. For this function, it was noticed that there are elements in the codomain that have no preimage or, equivalently, there are elements in the codomain that are not the image of any element in the domain. The set we are talking about is the subset of the codomain consisting of all images of the elements of the domain of the function, and it is called the range of the function.

Definition

Let $f : A \to B$. The set $\{f(x) \mid x \in A\}$ is called the ***range of the function*** f and is denoted by range (f). The range of f is sometimes called the ***image of the function*** f (or the ***image of*** A ***under*** f).

The range of $f : A \to B$ could equivalently be defined as follows:

$$\text{range}(f) = \{y \in B \mid y = f(x) \text{ for some } x \in A\}.$$

Notice that this means that range(f) $\subseteq$ codom(f) but does not necessarily mean that range(f) = codom(f). Whether we have this set equality or not depends on the function f. More about this will be explored in Section 6.3.

Progress Check 6.2 (Codomain and Range)

1. Let b be the function that assigns to each person his or her birthday (month and day).

   (a) What is the domain of this function?
   (b) What is a codomain for this function?
   (c) In Preview Activity 6.1.2, we determined that the following statement is true: For each day D of the year, there exists a person x such that $b(x) = D$. What does this tell us about the range of the function b? Explain.
2. Let s be the function that associates with each natural number the sum of its distinct natural number factors.

   (a) What is the domain of this function?
   (b) What is a codomain for this function?
   (c) In Preview Activity 6.1.2, we determined that the following statement is false:
   For each $m \in \mathbb{N}$, there exists a natural number n such that $s(n) = m$.
   Give an example of a natural number m that shows this statement is false, and explain what this tells us about the range of the function s.

Answer

Add texts here. Do not delete this text first.

The Graph of a Real Function

We will finish this section with methods to visually communicate information about two specific types of functions. The first is the familiar method of graphing functions that was a major part of some previous mathematics courses. For example, consider the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2 - 2x - 1$.

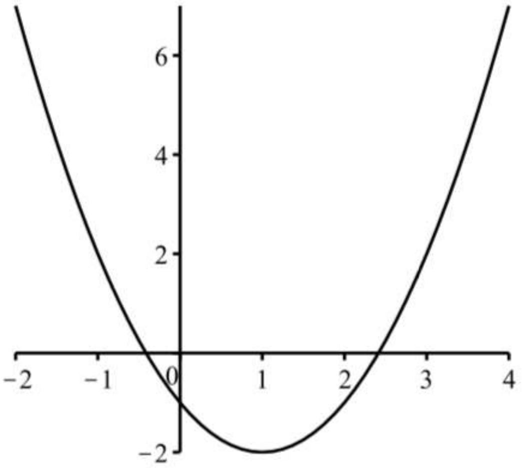


Figure 6.1: Graph of $y = g(x)$, where $g(x) = x^2 - 2x - 1$

Every point on this graph corresponds to an ordered pair (x, y) of real numbers, where $y = g(x) = x^2 - 2x - 1$. Because we use the Cartesian plane when drawing this type of graph, we can only use this type of graph when both the domain and the codomain of the function are subsets of the real numbers $\mathbb{R}$. Such a function is sometimes called a **real function**. The graph of a real function is a visual way to communicate information about the function. For example, the range of g is the set of all y-values that correspond to points on the graph. In this case, the graph of g is a parabola and has a vertex at the point (1, -2). (**Note**: The x-coordinate of the vertex can be found by using calculus and solving the equation $f\prime(x) = 0$.) Since the graph of the function g is a parabola, we know that pattern shown on the left end and the right end of the graph continues and we can conclude that the range of g is the set of all $y \in \mathbb{R}$ such that $y \geq -2$. That is,

$$\text{range}(g) = \{y \in \mathbb{R} \mid y \geq -2\}.$$

? Progress Check 6.3 (Using the Graph of a Real Function)

The graph in Figure 6.2 shows the graph of (slightly more than) two complete periods for a function $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = Asin(Bx)$ for some positive real number constants A and B.

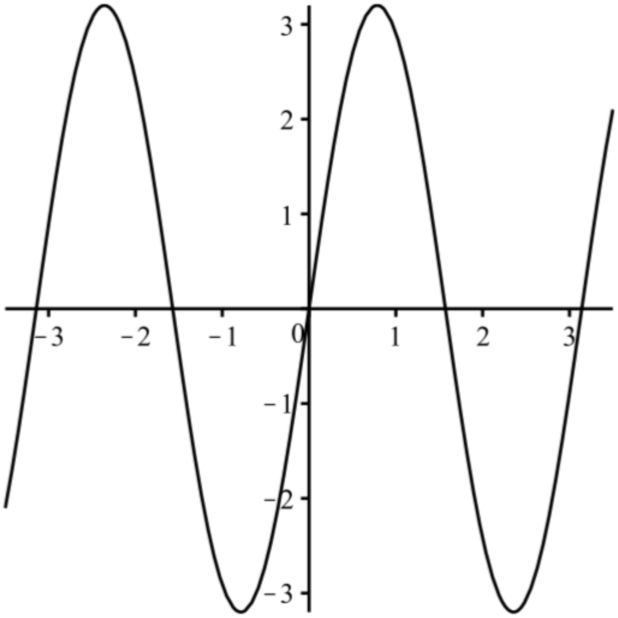


Figure 6.2: Graph of $y = f(x)$

1. We can use the graph to estimate the output for various inputs. This is done by estimating the y-coordinate for the point on the graph with a specified x-coordinate. On the graph, draw vertical lines at $x = -1$ and $x = 2$ and estimate the values of $f(-1)$ and $f(2)$.
2. Similarly, we can estimate inputs of the function that produce a specified output. This is done by estimating the x-coordinates of the points on the graph that have a specified y-coordinate. Draw a horizontal line at $y = 2$ and estimate at least two values of x such that $f(x) = 2$.
3. Use the graph Figure 6.2 to estimate the range of the function f.

Answer

Add texts here. Do not delete this text first.

Arrow Diagrams

Sometimes the domain and codomain of a function are small, finite sets. When this is the case, we can define a function simply by specifying the outputs for each input in the domain. For example, if we let $A = \{1, 2, 3\}$ and let $B = \{a, b\}$, we can define a function $F : A \to B$ by specifying that

$$F(1) = a, F(2) = a, \text{ and } F(3) = b.$$

This is a function since each element of the domain is mapped to exactly one element in B. A convenient way to illustrate or visualize this type of function is with a so-called **arrow diagram** as shown in Figure 6.3. An arrow diagram can

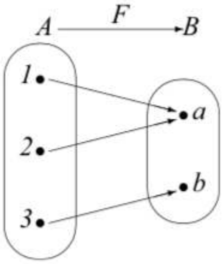


Figure 6.3: Arrow Diagram for a Function

be used when the domain and codomain of the function are finite (and small). We represent the elements of each set with points and then use arrows to show how the elements of the domain are associated with elements of the codomain. For example, the arrow from the point 2 in A to the point a in B represents the fact that $F(2) = a$. In this case, we can use the arrow diagram in Figure 6.3 to conclude that range(F)$= \{a, b\}$.

? Progress Check 6.4 (Working with Arrow Diagrams)

Let $A = \{1, 2, 3, 4\}$ and let $B = \{a, b, c\}$.

1. Which of the arrow diagrams in Figure 6.4 can be used to represent a function from A to B? Explain.
2. For those arrow diagrams that can be used to represent a function from A to B, determine the range of the function.

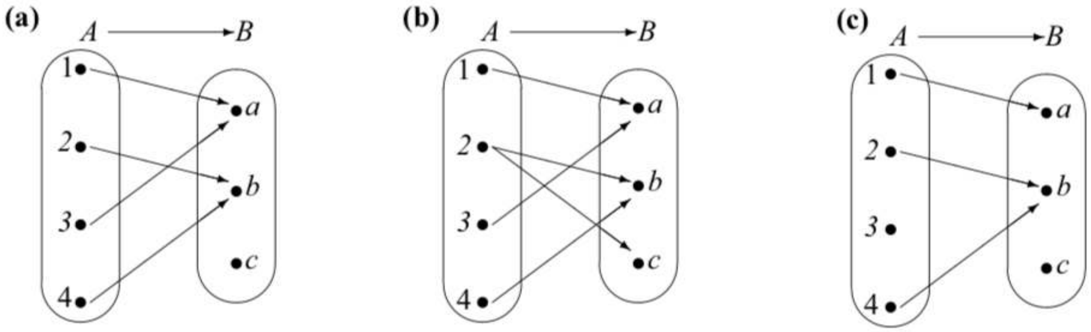


Figure 6.4: Arrow Diagram for a Function

Answer

Add texts here. Do not delete this text first.

? Exercises 6.1

1. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 - 2x$.

   (a) Evaluate $f(-3)$, $f(-1)$, $f(1)$, and $f(3)$.
   (b) Determine the set of all of the preimages of 0 and the set of all of the preimages of 4.
   (c) Sketch a graph of the function f.
   (d) Determine the range of the function f.

2. Let $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \geq 0\}$, and let $s : \mathbb{R} \to \mathbb{R}^*$ be defined by $s(x) = x^2$.

   (a) Evaluate $s(-3)$, $s(-1)$, $s(1)$, and $s(3)$.
   (b) Determine the set of all of the preimages of 0 and the set of all of the preimages of 2.
   (c) Sketch a graph of the function s.
   (d) Determine the range of the function s.
3. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(m) = 3 - m$.

   (a) Evaluate $f(-7)$, $f(-3)$, $f(3)$, and $f(7)$.
   (b) Determine the set of all of the preimages of 5 and the set of all of the preimages of 4.
   (c) Determine the range of the function f.
   (d) This function can be considered a real function since $\mathbb{Z} \subseteq \mathbb{R}$. Sketch a graph of this function. **Note**: The graph will be an infinite set of points that lie on a line. However, it will not be a line since its domain is not $\mathbb{R}$ but is $\mathbb{Z}$.
4. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(m) = 2m + 1$.

   (a) Evaluate $f(-7)$, $f(-3)$, $f(3)$, and $f(7)$.
   (b) Determine the set of all of the preimages of 5 and the set of all of the preimages of 4.
   (c) Determine the range of the function f.
   (d) Sketch a graph of the function f. See the comments in Exercise (3d).
5. Recall that a **real function** is a function whose domain and codomain are subsets of the real numbers R. (See page 288.) Most of the functions used in calculus are real functions. Quite often, a real function is given by a formula or a graph with no specific reference to the domain or the codomain. In these cases, the usual convention is to assume that the domain of the real function f is the set of all real numbers x for which $f(x)$ is a real number, and that the codomain is $\mathbb{R}$. For example, if we define the (real) function f by

   $$f(x) = \frac{x}{x-2}, \tag{6.1.5}$$

   we would be assuming that the domain is the set of all real numbers that are not equal to 2 and that the codomain in $\mathbb{R}$. Determine the domain and range of each of the following real functions. It might help to use a graphing calculator to plot a graph of the function.

   (a) The function k defined by $k(x) = \sqrt{x-3}$
   (b) The function F defined by $F(x) = ln(2x-1)$
   (c) The function f defined by $f(x) = 3sin(2x)$
   (d) The function g defined by $g(x) = \dfrac{4}{x^2-4}$
   (e) The function G defined by $G(x) = 4cos(\pi x) + 8$
6. **The number of divisors function**. Let d be the function that associates with each natural number the number of its natural number divisors. That is $d : \mathbb{N} \to \mathbb{N}$ where $d(n)$ is the number of natural number divisors of n. For example, $d(6) = 4$ since 1, 2, 3, and 6 are the natural number divisors of 6.

   (a) Calculate $d(k)$ for each natural number k from 1 through 12.
   (b) Does there exist a natural number n such that $d(n) = 1$? What is the set of preimages of the natural number 1.
   (c) Does there exist a natural number n such that $d(n) = 2$? If so, determine the set of all preimages of the natural number 2.
   (d) Is the following statement true or false? Justify your conclusion.
   For all $m, n \in \mathbb{N}$, if $m \neq n$, then $d(m) \neq d(n)$.
   (e) Calculate $d(2^k)$ for $k = 0$ and for each natural number k from 1 through 6.
   (f) Based on your work in Exercise (6e), make a conjecture for a formula for $d(2^n)$ where n is a nonnegative integer. Then explain why your conjecture is correct.
   (g) Is the following statement is true or false?
   For each $n \in \mathbb{N}$, there exists a natural number m such that $d(m) = n$.

7. In Exercise (6), we introduced the **number of divisors function** d. For this function, $d : \mathbb{N} \to \mathbb{N}$, where $d(n)$ is the number of natural number divisors of n.
   A function that is related to this function is the so-called **set of divisors function**. This can be defined as a function S that associates with each natural number the set of its distinct natural number factors. For example, $S(6) = \{1, 2, 3, 6\}$ and $S(10) = \{1, 2, 5, 10\}$.

   (a) Discuss the function S by carefully stating its domain, codomain, and its rule for determining outputs.
   (b) Determine $S(n)$ for at least five different values of n.
   (c) Determine $S(n)$ for at least three different prime number values of n.
   (d) Does there exist a natural number n such that card($S(n) = 1$)? Explain. [Recall that card($S(n)$) is the number of elements in the set $S(n)$.]
   (e) Does there exist a natural number n such that card($S(n) = 2$)? Explain.
   (f) Write the output for the function d in terms of the output for the function S. That is, write $d(n)$ in terms of $S(n)$.
   (g) Is the following statement true or false? Justify your conclusion.
   For all natural numbers m and n, if $m \neq n$, then $S(m) \neq S(n)$.
   (h) Is the following statement true or false? Justify your conclusion.
   For all sets T that are subsets of $\mathbb{N}$, there exists a natural number n such that $S(n) = T$.

   Explorations and Activities
8. Creating Functions with Finite Domains. Let $A = \{a, b, c, d\}$, $B = \{a, b, c\}$. and $C = \{s, t, u, v\}$. In each of the following exercises, draw an arrow diagram to represent your function when it is appropriate.

   (a) Create a function $f : A \to C$ whose range is the set C or explain why it is not possible to construct such a function.
   (b) Create a function $f : A \to C$ whose range is the set $\{u, v\}$ or explain why it is not possible to construct such a function.
   (c) Create a function $f : B \to C$ whose range is the set C or explain why it is not possible to construct such a function.
   (d) Create a function $f : A \to C$ whose range is the set $\{u\}$ or explain why it is not possible to construct such a function.
   (e) If possible, create a function $f : A \to C$ that satisfies the following condition:
   For all $x, y \in A$, if $x \neq y$, then $f(x) \neq f(y)$.
   If it is not possible to create such a function, explain why.
   (f) If possible, create a function $f : A \to \{s, t, u\}$ that satisfies the following condition:
   For all $x, y \in A$, if $x \neq y$, then $f(x) \neq f(y)$.
   If it is not possible to create such a function, explain why.

Answer

Add texts here. Do not delete this text first.

This page titled 6.1: Introduction to Functions is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

6.2: More about Functions

In Section 6.1, we have seen many examples of functions. We have also seen various ways to represent functions and to convey information about them. For example, we have seen that the rule for determining outputs of a function can be given by a formula, a graph, or a table of values. We have also seen that sometimes it is more convenient to give a verbal description of the rule for a function. In cases where the domain and codomain are small, finite sets, we used an arrow diagram to convey information about how inputs and outputs are associated without explicitly stating a rule. In this section, we will study some types of functions, some of which we may not have encountered in previous mathematics courses.

? Preview Activity $6.2.1$: The Number of Diagonals of a Polygon

A **polygon** is a closed plane figure formed by the joining of three or more straight lines. For example, a triangle is a polygon that has three sides; a **quadrilateral** is a polygon that has four sides and includes squares, rectangles, and parallelograms; a **pentagon** is a polygon that has five sides; and an **octagon** is a polygon that has eight sides. A r**egular polygon** is one that has equal-length sides and congruent interior angles.

A **diagonal of a polygon** is a line segment that connects two nonadjacent vertices of the polygon. In this activity, we will assume that all polygons are **convex polygons** so that, except for the vertices, each diagonal lies inside the polygon. For example, a triangle (3-sided polygon) has no diagonals and a rectangle has two diagonals.

1. How many diagonals does any quadrilateral (4-sided polygon) have?
2. Let $D = \mathbb{N} - \{1, 2\}$. Define $d : D \to \mathbb{N} \cup \{0\}$ so that $d(n)$ is the number of diagonals of a convex polygon with n sides. Determine the values of $d(3)$, $d(4)$, $d(5)$, $d(6)$, $d(7)$, and $d8)$. Arrange the results in the form of a table of values for the function d.
3. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by

$$f(x) = \frac{x(x-3)}{2}. \tag{6.2.1}$$

   Determine the values of $f(0)$, $f(1)$, $f(2)$, $f(3)$, $f(4)$, $f(5)$, $f(6)$, $f(7)$, $f(8)$, and $f9)$. Arrange the results in the form of a table of values for the function f.
4. Compare the functions in Parts (2) and (3). What are the similarities between the two functions and what are the differences? Should these two functions be considered equal functions? Explain.

? Preview Activity $6.2.1$: Derivatives

In calculus, we learned how to find the derivatives of certain functions. For example, if $f(x) = x^2(sinx)$, then we can use the product rule to obtain

$$f\prime(x) = 2x(\sin x) + x^2(\cos x). \tag{6.2.2}$$

1. If possible, find the derivative of each of the following functions:

   (a) $f(x) = x^4 - 5x^3 + 3x - 7$
   (b) $g(x) = \cos(5x)$
   (c) $h(x) = \dfrac{\sin x}{x}$
   (d) $k(x) = e^{-x^2}$
   (e) $r(x) = |x|$
2. Is it possible to think of differentiation as a function? Explain. If so, what would be the domain of the function, what could be the codomain of the function, and what is the rule for computing the element of the codomain (output) that is associated with a given element of the domain (input)?

Functions Involving Congruences

Theorem 3.31 and Corollary 3.32 state that an integer is congruent (mod n) to its remainder when it is divided by n. (Recall that we always mean the remainder guaranteed by the Division Algorithm, which is the least nonnegative remainder.) Since this remainder is unique and since the only possible remainders for division by n are 0, 1, 2, ..., $n-1$, we then know that each integer is congruent, modulo n, to precisely one of the integers 0, 1, 2, ..., $n-1$. So for each natural number n, we will define a new set $\mathbb{Z}_n$ as follows:

$$\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}.$$

For example, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ and $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. We will now explore a method to define a function from $\mathbb{Z}_6$ to $\mathbb{Z}_6$.

For each $x \in \mathbb{Z}_6$, we can compute $x^2 + 3$ and then determine the value of r in $\mathbb{Z}_6$ so that

$$(x^2 + 3) \equiv r \text{ (mod 6)}.$$

Since r must be in $\mathbb{Z}_6$, we must have $0 \le r < 6$. The results are shown in the following table.

Table6 .1: Table of Values Defined by a Congruence

x	r, where $x^2+3) \equiv r(\text{mod } 6)$	x	r, where $x^2+3) \equiv r(\text{mod } 6)$
0	3	3	0
1	4	4	1
2	1	5	4

The value of x in the first column can be thought of as the input for a function with the value of r in the second column as the corresponding output. Each input produces exactly one output. So we could write

$$f : \mathbb{Z}_6 \to \mathbb{Z}_6 \text{ by } f(x) = r \text{ where } (x^2+3) \equiv r \text{ (mod 6)}.$$

This description and the notation for the outputs of this function are quite cumbersome. So we will use a more concise notation. We will, instead, write

Let $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ by $f(x) = (x^2+3)$ (mod 6).

? Progress Check 6.5 (Functions Defined by Congruences)

Let $\mathbb{Z}_6 = \{0, 1, 2, 3, 4\}$. Define

$$f : \mathbb{Z}_5 \to \mathbb{Z}_5 \text{ by } f(x) = x^4 \text{ (mod 5), for each } x \in \mathbb{Z}_5;$$

$$g : \mathbb{Z}_5 \to \mathbb{Z}_5 \text{ by } g(x) = x^5 \text{ (mod 5), for each } x \in \mathbb{Z}_5;$$

1. Determine $f(0)$, $f(1)$, $f(2)$, $f(3)$, and $f(4)$ and represent the function f with an arrow diagram.
2. Determine $g(0)$, $g(1)$, $g(2)$, $g(3)$, and $g(4)$ and represent the function g with an arrow diagram.

Answer

Add texts here. Do not delete this text first.

Equality of Functions

The idea of equality of functions has been in the background of our discussion of functions, and it is now time to discuss it explicitly. The preliminary work for this discussion was Preview Activity 6.2.1, in which $D = \mathbb{N} - \{1, 2\}$ and there were two functions:

- $d : D \to \mathbb{N} \cup \{0\}$, where $d(n)$ is the number of diagonals of a convex polygon with n sides
- $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = \dfrac{x(x-3)}{2}$, for each real number x.

In Preview Activity 6.2.1, we saw that these two functions produced the same outputs for certain values of the input (independent variable). For example, we can verify that

$$d(3) = f(3) = 0,\ d(4) = f(4) = 2,$$
$$d(5) = f(5) = 5, \text{ and } d(6) = f(6) = 9.$$

Although the functions produce the same outputs for some inputs, these are two different functions.For example, the outputs of the function f are determined by a formula, and the outputs of the function d are determined by a verbal description. This is not enough, however, to say that these are two different functions. Based on the evidence from Preview Activity $6.2.1$, we might make the following conjecture:

$$\text{For } n \geq 3,\ d(n) = \frac{n(n-3)}{2}.$$

Although we have not proved this statement, it is a true statement. (See Exercise 6.) However, we know the function d and the function f are not the same function. For example,

- $f(0) = 0$, but 0 is not in the domain of d;
- $f(\pi) = \frac{\pi(\pi-3)}{2}$, but π is not in the domain of d.

We thus see the importance of considering the domain and codomain of each of the two functions in determining whether the two functions are equal or not. This motivates the following definition.

Definition: equal Functions

Two functions f and g are **equal** provided that

- The domain of f equals the domain of g. That is dom(f) = dom(g)
- The codomain of f equals the codomain of g. That is codom(f) = codom(g)
- For each x in the domain of f (which equals the domain of g), $f(x) = g(x)$.

Progress Check 6.6: Equality of Functions

Let A be a nonempty set. The **identity function on the set** A, denoted by I_A, is the function $I_A : A \to A$ defined by $I_A(x) = x$ for every x in A. That is, for the identity map, the output is always equal to the input.

For this progress check, we will use the functions f and g from Progress Check 6.5. The identity function on the set $\mathbb{Z}_5$ is

$I_{\mathbb{Z}_5} : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $I_{\mathbb{Z}_5}(x) = x$ (mod 5), for each $x \in \mathbb{Z}_5$.

Is the identity function on $\mathbb{Z}_5$ equal to either of the functions f or g from Progress Check 6.5? Explain.

Answer

Add texts here. Do not delete this text first.

Mathematical Processes as Functions

Certain mathematical processes can be thought of as functions. In Preview Activity $6.2.2$, we reviewed how to find the derivatives of certain functions, and we considered whether or not we could think of this differentiation process as a function. If we use a differentiable function as the input and consider the derivative of that function to be the output, then we have the makings of a function. Computer algebra systems such as *Maple and Mathematica* have this derivative function as one of their predefined operators.

Following is some *Maple* code (using the Classic Worksheet version of *Maple*) that can be used to find the derivative function of the function given by $f(x) = x^2(sinx)$. The lines that start with the *Maple* prompt, [>, are the lines typed by the user. The centered lines following these show the resulting *Maple* output. The first line defines the function f, and the second line uses the derivative function D to produce the derivative of the function f.

[> f := x → x^2 ∗ sin (x);

$$f := x \to x^2 \sin(x)$$

[> f1 := D(f);

$$f1 := x \to 2x \sin(x) + x^2 \cos(x)$$

We must be careful when determining the domain for the derivative function since there are functions that are not differentiable. To make things reasonably easy, we will let F be the set of all real functions that are differentiable and call this the domain of the derivative function D. We will use the set T of all real functions as the codomain. So our function D is

$$D : F \to T \text{ by } D(f) = f\prime.$$

Progress Check 6.7: Average of a Finite Set of Numbers

Let $A = \{a_1, a_2, ...a_n\}$ be a finite set whose elements are the real numbers $a_1, a_2, ...a_n$. We define the **average of the set** A to be the real number $\bar{A}$, where

$$\bar{A} = \frac{a_1, a_2, ...a_n}{n}.$$

1. Find the average of $A = \{3, 7, -1, 5\}$.
2. Find the average of $B = \{7, -2, 3.8, 4.2, 7.1\}$.
3. Find the average of $C = \{\sqrt{2}, \sqrt{3}, \pi - \sqrt{3}\}$.
4. Now let $\mathcal{F}(\mathbb{R})$ be the set of all finite subsets of $\mathbb{R}$. That is, a subset A of $\mathbb{R}$ is in $\mathcal{F}(\mathbb{R})$ if and only if A contains only a finite number of elements. Carefully explain how the process of finding the average of a finite subset of $\mathbb{R}$ can be thought of as a function. In doing this, be sure to specify the domain of the function and the codomain of the function.

Answer

Add texts here. Do not delete this text first.

Sequences as Functions

A sequence can be considered to be an infinite list of objects that are indexed (subscripted) by the natural numbers (or some infinite subset of $\mathbb{N} \cup \{0\}$). Using this idea, we often write a sequence in the following form:

$$a_1, a_2, ..., a_n, ...$$

In order to shorten our notation, we will often use the notation $\langle a_n \rangle$ to represent this sequence. Sometimes a formula can be used to represent the terms of a sequence, and we might include this formula as the nth term in the list for a sequence such as in the following example:

$$1, \frac{1}{2}, \frac{1}{3}, ..., \frac{1}{n}, ...$$

In this case, the nth term of the sequence is $\frac{1}{n}$. If we know a formula for the nth term, we often use this formula to represent the sequence. For example, we might say

$$\text{Define the sequence } \langle a_n \rangle \text{ by } a_n = \frac{1}{n} \text{ for each } n \in \mathbb{N}.$$

This shows that this sequence is a function with domain $\mathbb{N}$. If it is understood that the domain is $\mathbb{N}$, we could refer to this as the sequence $\langle \frac{1}{n} \rangle$. Given an element of the domain, we can consider a_n to be the output. In this case, we have used subscript notation to indicate the output rather than the usual function notation. We could just as easily write

$$a(n) = \frac{1}{n} \text{ instead of } a_n = \frac{1}{n}.$$

We make the following formal definition.

Definition: sequence

An (infinite) **sequence** is a function whose domain is $\mathbb{N}$ or some infinite subset of $\mathbb{N} \cup \{0\}$.

Progress Check 6.8 (Sequences)

Find the sixth and tenth terms of each of the following sequences:

1. $\frac{1}{3}, \frac{1}{6}, \frac{1}{9}, \frac{1}{12}, \cdots$
2. $\langle a_n \rangle$, where $a_n = \frac{1}{n^2}$ for each $n \in \mathbb{N}$
3. $\langle (-1)^n \rangle$

Answer

Add texts here. Do not delete this text first.

Functions of Two Variables

In Section 5.4, we learned how to form the Cartesian product of two sets. Recall that a Cartesian product of two sets is a set of ordered pairs. For example, the set $\mathbb{Z} \times \mathbb{Z}$ is the set of all ordered pairs, where each coordinate of an ordered pair is an integer. Since a Cartesian product is a set, it could be used as the domain or codomain of a function. For example, we could use $\mathbb{Z} \times \mathbb{Z}$ as the domain of a function as follows:

Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be defined by $f(m, n) = 2m + n$.

- Technically, an element of $\mathbb{Z} \times \mathbb{Z}$ is an ordered pair, and so we should write $f((m, n))$ for the out put of the function f when the input is the ordered pair (m, n). However, the double parentheses seem unnecessary in this context and there should be no confusion if we write $f(m, n)$ for the output of the function f when the input is (m, n). So, for example, we simply write

$$\begin{aligned} f(3,2) &= 2 \cdot 3 + 2 = 8, \text{ and} \\ f(-4,5) &= 2 \cdot (-4) + 5 = -3. \end{aligned} \tag{6.2.3}$$

- Since the domain of this function is $\mathbb{Z} \times \mathbb{Z}$ and each element of $\mathbb{Z} \times \mathbb{Z}$ is an ordered pair of integers, we frequently call this type of function a **function of two variables.**

Finding the preimages of an element of the codomain for the function f, $\mathbb{Z}$, usually involves solving an equation with two variables. For example, to find the preimages of 0 2 Z, we need to find all ordered pairs $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ such that $f(m, n) = 0$. This means that we must find all ordered pairs $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ such that

$$2m + n = 0$$

Three such ordered pairs are (0,0), (1, -2), and (-1, 2). In fact, whenever we choose an integer value for m, we can find a corresponding integer n such that $2m + n = 0$. This means that 0 has infinitely many preimages, and it may be difficult to specify the set of all of the preimages of 0 using the roster method. One way that can be used to specify this set is to use set builder notation and say that the following set consists of all of the preimages of 0:

$$\{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid 2m + n = 0\} = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid n = -2m\}.$$

The second formulation for this set was obtained by solving the equation $2m + n = 0$ for n.

? Progress Check 6.9 (Working with a Function of Two Variables)

Let $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be defined by $g(m, n) = m^2 - n$ for all $(m, n) \in \mathbb{Z} \times \mathbb{Z}$.

1. Determine $g(0, 3)$, $g(3, -2)$, $g(-3, -2)$, and $g(7, -1)$.
2. Determine the set of all preimages of the integer 0 for the function g. Write your answer using set builder notation.
3. Determine the set of all preimages of the integer 5 for the function g. Write your answer using set builder notation.

Answer

Add texts here. Do not delete this text first.

? Exercise 6.2

1. Let $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Define $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $f(x) = x^2 + 4$ (mod 5) and define $g : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $g(x) = (x + 1)(x + 4)$ (mod 5).

   (a) Calculate $f(0)$, $f(1)$, $f(2)$, $f(3)$, and $f(4)$.
   (b) Calculate $g(0)$, $g(1)$, $g(2)$, $g(3)$, and $g(4)$.
   (c) Is the function f equal to the function g? Explain.
2. Let $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Define $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $f(x) = x^2 + 4$ (mod 5) and define $g : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $g(x) = (x + 1)(x + 4)$ (mod 5).

   (a) Calculate $f(0)$, $f(1)$, $f(2)$, $f(3)$, and $f(4)$.
   (b) Calculate $g(0)$, $g(1)$, $g(2)$, $g(3)$, and $g(4)$.
   (c) Is the function f equal to the function g? Explain.

3. Let $f : (\mathbb{R} - \{0\}) \to \mathbb{R}$ by $f(x) = \dfrac{x^3 + 5x}{x}$ and let $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^2 + 5$.

   (a) Calculate $f(2)$, $f(-2)$, $f(3)$, and $f(\sqrt{2})$.
   (b) Calculate $g(0)$, $g(2)$, $g(-2)$, $g(3)$, and $g(\sqrt{2})$.
   (c) Is the function f equal to the function g? Explain.
   (d) Now let $h : (\mathbb{R} - \{0\}) \to \mathbb{R}$ by $h(x) = x^2 + 5$. Is the function f equal to the function h? Explain.
4. Represent each of the following sequences as functions. In each case, state the domain, codomain, and rule for determining the outputs of the function. Also, determine if any of the sequences are equal.

   (a) $1, \frac{1}{4}, \frac{1}{9}, \frac{1}{16}, \ldots$
   (b) $\frac{1}{3}, \frac{1}{9}, \frac{1}{27}, \frac{1}{81}, \ldots$
   (c) 1, -1, 1, -1, 1, -1, ...
   (d) cos(0), cos(π), cos(2π), cos(3π), cos(4π), ...
5. Let A and B be two nonempty sets. There are two **projection functions** with domain $A \times B$, the Cartesian product of A and B. One projection function will map an ordered pair to its first coordinate, and the other projection function will map the ordered pair to its second coordinate. So we define
   $p_1 : A \times B \to A$ by $p_1(a, b) = a$ for every $(a, b) \in A \times B$; and
   $p_2 : A \times B \to B$ by $p_2(a, b) = a$ for every $(a, b) \in A \times B$.
   Let $A = \{1, 2\}$ and let $B = \{x, y, z\}$.

   (a) Determine the outputs for all possible inputs for the projection function$p_1 : A \times B \to A$.
   (b) Determine the outputs for all possible inputs for the projection function$p_2 : A \times B \to B$.
   (c) What is the range of these projection functions?
   (d) Is the following statement true or false? Explain.
   For all $(m, n), (u, v) \in A \times B$, if $(m, n) \neq (u, v)$, then
   $p_1(m, n) \neq p_1(u, v)$.
6. Let $D = \mathbb{N} - \{1, 2\}$ and define $d : D \to \mathbb{N} \cup \{0\}$ by $d(n) =$ the number of diagonals of a convex polygon with n sides. In Preview Activity 6.2.1, we showed that for values of n from 3 through 8,

$$d(n) = \frac{n(n-3)}{2}. \tag{6.2.4}$$

   Use mathematical induction to prove that for all $n \in D$,

$$d(n) = \frac{n(n-3)}{2}. \tag{6.2.5}$$

   Hint: To get an idea of how to handle the inductive step, use a pentagon. First, form all the diagonals that can be made from four of the vertices. Then consider how to make new diagonals when the fifth vertex is used. This may generate an idea of how to proceed from a polygon with k sides to a polygon with $k + 1$ sides.
7. Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be defined by $f(m, n) = m + 3n$.

   (a) Calculate $f(-3, 4)$ and $f(-2, -7)$.
   (b) Determine the set of all the preimages of 4 by using set builder notation to describe the set of all $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ such that $f(m, n) = 4$.
8. Let $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be defined by $g(m, n) = (2m, m - n)$.

   (a) Calculate $g(3, 5)$ and $g(-1, 4)$.
   (b) Determine all the preimages of .0; 0/. That is, find all $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ such that $g(m, n) = (0, 0)$.
   (c) Determine the set of all the preimages of (8, -3).
   (d) Determine the set of all the preimages of (1, 1).

(e) Is the following proposition true or false? Justify your conclusion.
For each $(s,t) \in \mathbb{Z} \times \mathbb{Z}$, there exists an $(m,n) \in \mathbb{Z} \times \mathbb{Z}$ such that $g(m,n) = (s,t)$.

9. A **2 by 2 matrix over** $\mathbb{R}$ is a rectangular array of four real numbers arranged in two rows and two columns. We usually write this array inside brackets (or parentheses) as follows:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{6.2.6}$$

where a, b, c and d are real numbers. The **determinant** of the 2 by 2 matrix A, denoted by det(A), is defined as det(A) = $ad - bc$.

(a) Calculate the determinant of each of the following matrices:
$\begin{bmatrix} 3 & 5 \\ 4 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & 7 \end{bmatrix}$, and $\begin{bmatrix} 3 & -2 \\ 5 & 0 \end{bmatrix}$.
(b) Let $\mathcal{M}_2(\mathbb{R})$ be the set of all 2 by 2 matrices over $\mathbb{R}$. The mathematical process of finding the determinant of a 2 by 2 matrix over $\mathbb{R}$ can be thought of as a function. Explain carefully how to do so, including a clear statement of the domain and codomain of this function.

10. Using the notation from Exercise (9), let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{6.2.7}$$

be a 2 by 2 matrix over $\mathbb{R}$. The transpose of the matrix A, denoted by A^T, is the 2 by 2 matrix over $\mathbb{R}$ defined by

$$A^T = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \tag{6.2.8}$$

(a) Calculate the transpose of each of the following matrices:
$\begin{bmatrix} 3 & 5 \\ 4 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & 7 \end{bmatrix}$, and $\begin{bmatrix} 3 & -2 \\ 5 & 0 \end{bmatrix}$.
(b) Let $\mathcal{M}_2(\mathbb{R})$ be the set of all 2 by 2 matrices over $\mathbb{R}$. The mathematical process of finding the determinant of a 2 by 2 matrix over $\mathbb{R}$ can be thought of as a function. Explain carefully how to do so, including a clear statement of the domain and codomain of this function.

Explorations and Activities

11. **Integration as a Function.** In calculus, we learned that if f is real function that is continuous on the closed interval [a, b], then the definite integral $\int_a^b f(x)dx$ is a real number. In fact, one form of the **Fundamental Theorem of Calculus** states that

$$\int_a^b f(x)dx = F(b) - F(a), \tag{6.2.9}$$

where F is any antiderivative of f, that is, where $F\prime = f$.

(a) Let [a, b] be a closed interval of real numbers and let $C[a,b]$ be the set of all real functions that are continuous on [a, b]. That is,

$$C[a,b] = \{f : [a,b] \to \mathbb{R} \mid f \text{ is continuous on } [a,b]\}. \tag{6.2.10}$$

i. Explain how the definite integral $\int_a^b f(x)dx$ can be used to define a function I from $C[a,b]$ to $\mathbb{R}$.
ii. Let $[a,b] = [0,2]$. Calculate $I(f)$, where $f(x) = x^2 + 1$.
iii. Let $[a,b] = [0,2]$. Calculate $I(g)$, where $g(x) = sin(\pi x)$.

In calculus, we also learned how to determine the indefinite integral $\int f(x)dx$ of a continuous funtion f.

(b) Let $f(x) = x^2 + 1$ and $g(x) = cos(2x)$. Determine $\int f(x)dx$ and $\int g(x)dx$.
(c) Let f be a continuous function on the closed interval [0, 1] and let T be the set of all real functions. Can the process of determining the indefinite integral of a continuous function be used to define a function from $C[0,1]$ to T? Explain.
(d) Another form of the Fundamental Theorem of Calculus states that if f is continuous on the interval [a, b] and if

$$g(x) = \int_a^x f(t)dt \tag{6.2.11}$$

For each x in [a, b], then $g\prime(x) = f(x)$. That is, g is an antiderivative of f. Explain how this t heorem can be used to define a function from $C[a,b]$ to T, where the output of the function i s an antiderivative of the input. (Recall that T is the set of all real functions.)

Answer

Add texts here. Do not delete this text first.

This page titled 6.2: More about Functions is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

6.3: Injections, Surjections, and Bijections

Functions are frequently used in mathematics to define and describe certain relationships between sets and other mathematical objects. In addition, functions can be used to impose certain mathematical structures on sets. In this section, we will study special types of functions that are used to describe these relationships that are called injections and surjections. Before defining these types of functions, we will revisit what the definition of a function tells us and explore certain functions with finite domains.

? Preview Activity $6.3.1$: Functions with Finite Domains

Let A and B be sets. Given a function $f : A \to B$, we know the following:

- For every $x \in A$, $f(x) \in B$. That is, every element of A is an input for the function f. This could also be stated as follows: For each $x \in A$, there exists a $y \in B$ such that $y = f(x)$.
- For a given $x \in A$, there is exactly one $y \in B$ such that $y = f(x)$.

The definition of a function does not require that different inputs produce different outputs. That is, it is possible to have $x_1, x_2 \in A$ with $x1 \neq x_2$ and $f(x_1) = f(x_2)$. The arrow diagram for the function f in Figure 6.5 illustrates such a function.

Also, the definition of a function does not require that the range of the function must equal the codomain. The range is always a subset of the codomain, but these two sets are not required to be equal. That is, if $g : A \to B$, then it is possible to have a $y \in B$ such that $g(x) \neq y$ for all $x \in A$. The arrow diagram for the function g in Figure 6.5 illustrates such a function.

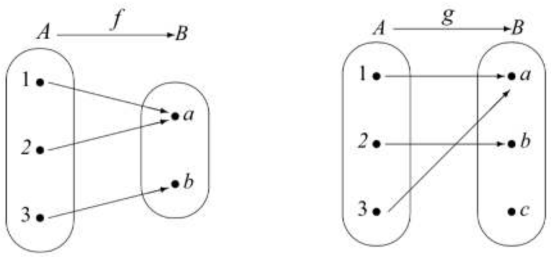
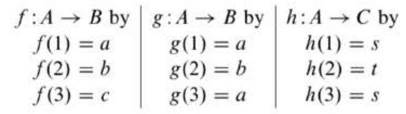


Figure 6.5: Arrow Diagram for Two Functions

Now let $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$, and $C = \{s, t\}$. Define



$f : A \to B$ by	$g : A \to B$ by	$h : A \to C$ by
$f(1) = a$	$g(1) = a$	$h(1) = s$
$f(2) = b$	$g(2) = b$	$h(2) = t$
$f(3) = c$	$g(3) = a$	$h(3) = s$

1. Which of these functions satisfy the following property for a function F?
   For all $x, y \in \text{dom}(F)$, if $x \neq y$, then $F(x) \neq F(y)$.
2. Which of these functions satisfy the following property for a function F?
   For all $x, y \in \text{dom}(F)$, if $F(x) = F(y)$, then $x = y$.
3. Determine the range of each of these functions.
4. Which of these functions have their range equal to their codomain?
5. Which of the these functions satisfy the following property for a function F?
   For all y in the codomain of F, there exists an $x \in \text{dom}(F\backslash)$ such that $F(x) = y$.

? Preview Activity $6.3.1$: Statements Involving Functions

Let A and B be nonempty sets and let $f : A \to B$. In Preview Activity $6.3.1$, we determined whether or not certain functions satisfied some specified properties. These properties were written in the form of statements, and we will now examine these statements in more detail.

1. Consider the following statement:
   For all $x, y \in A$, if $x \neq y$, then $f(x) \neq f(y)$.

   (a) Write the contrapositive of this conditional statement.
   (b) Write the negation of this conditional statement.
2. Now consider the statement:
   For all $y \in B$, there exists an $x \in A$ such that $f(x) = y$.
   Write the negation of this statement.
3. Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = 5x + 3$, for all $x \in \mathbb{R}$. Complete the following proofs of the following propositions about the function g.

   Proposition 1. For all $a, b \in \mathbb{R}$, if $g(a) = g(b)$, then $a = b$.
   Proof. We let $a, b \in \mathbb{R}$, and we assume that $g(a) = g(b)$ and will prove that $a = b$. Since $g(a) = g(b)$, we know that

   $$5a + 3 = 5b + 3. \tag{6.3.1}$$

   (Now prove that in this situation, $a = b$.)

   Proposition 2. For all $b \in \mathbb{R}$, there exists an $a \in \mathbb{R}$ such that $g(a) = b$.
   Proof. We let $b \in \mathbb{R}$. We will prove that there exists an $a \in \mathbb{R}$ such that $g(a) = b$ by constructing such an a in $\mathbb{R}$. In order for this to happen, we need $g(a) = 5a + 3 = b$.
   (Now solve the equation for a and then show that for this real number a, $g(a) = b$.)

Injections

In previous sections and in Preview Activity 6.3.1, we have seen examples of functions for which there exist different inputs that produce the same output. Using more formal notation, this means that there are functions $f : A \to B$ for which there exist $x_1, x_2 \in A$ with $x_1 \neq x_2$ and $f(x_1) = f(x_2)$. The work in the preview activities was intended to motivate the following definition.

Definition

Let $f : A \to B$ be a function from the set A to the set B. The function f is called an **injection** provided that

for all $x_1, x_2 \in A$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$.

When f is an injection, we also say that f is a **one-to-one function**, or that f is an **injective function.**

Notice that the condition that specifies that a function f is an injection is given in the form of a conditional statement. As we shall see, in proofs, it is usually easier to use the contrapositive of this conditional statement. Although we did not define the term then, we have already written the contrapositive for the conditional statement in the definition of an injection in Part (1) of Preview Activity 6.3.2. In that preview activity, we also wrote the negation of the definition of an injection. Following is a summary of this work giving the conditions for f being an injection or not being an injection.

Let $f : A \to B$

"The function f is an injection" means that

- for all $x_1, x_2 \in A$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$; or
- for all $x_1, x_2 \in A$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

“The function f is not an injection” means that

- There exist $x_1, x_2 \in A$ such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$.

Progress Check 6.10 (Working with the Definition of an Injection)

Now that we have defined what it means for a function to be an injection, we can see that in Part (3) of Preview Activity 6.3.2, we proved that the function $g : \mathbb{R} \to \mathbb{R}$ is an injection, where $g(x/) = 5x + 3$ for all $x \in \mathbb{R}$. Use the definition (or its negation) to determine whether or not the following functions are injections.

1. $k : A \to B$, where $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, and $k(a) = 4$, $k(b) = 1$, and $k(c) = 3$.
2. $f : A \to C$, where $A = \{a, b, c\}$, $C = \{1, 2, 3\}$, and $f(a) = 2$, $f(b) = 3$, and $f(c) = 2$.
3. $F : \mathbb{Z} \to \mathbb{Z}$ defined by $F(m) = 3m + 2$ for all $m \in \mathbb{Z}$
4. $h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = x^2 - 3x$ for all $x \in \mathbb{R}$
5. $s : \mathbb{Z}_5 \to \mathbb{Z}_5$ defined by $sx) = x^3$ for all $x \in \mathbb{Z}_5$

Answer

Add texts here. Do not delete this text first.

Surjections

In previous sections and in Preview Activity 6.3.1, we have seen that there exist functions $f : A \to B$ for which range$(f) = B$. This means that every element of B is an output of the function f for some input from the set A. Using quantifiers, this means that for every $y \in B$, there exists an $x \in A$ such that $f(x) = y$. One of the objectives of the preview activities was to motivate the following definition.

Definition

Let $f : A \to B$ be a function from the set A to the set B. The function f is called a **surjection** provided that the range of f equals the codomain of f. This means that

for every $y \in B$, there exists an $x \in A$ such that $f(x) = y$.

When f is a surjection, we also say that f is an **onto function** or that f maps A onto B. We also say that f is a **surjective function.**

One of the conditions that specifies that a function f is a surjection is given in the form of a universally quantified statement, which is the primary statement used in proving a function is (or is not) a surjection. Although we did not define the term then, we have already written the negation for the statement defining a surjection in Part (2) of Preview Activity 6.3.2. We now summarize the conditions for f being a surjection or not being a surjection.

Let $f : A \to B$

"The function f is a surjection" means that

- range(f) = codom$(f) = B$; or
- For every $y \in B$, there exsits an $x \in A$ such that $f(x) = y$.

“The function f is not a surjection” means that

- rang(f) \ne codom(f); or
- There exists a $y \in B$ such that for all $x \in A$, $f(x) \neq y$.

One other important type of function is when a function is both an injection and surjection. This type of function is called a bijection.

Definition

A **bijection** is a function that is both an injection and a surjection. If the function f is a bijection, we also say that f is **one-to-one and onto** and that f is a **bijective function.**

Progress Check 6.11 (Working with the Definition of a Surjection)

Now that we have defined what it means for a function to be a surjection, we can see that in Part (3) of Preview Activity $6.3.2$, we proved that the function $g : \mathbb{R} \to \mathbb{R}$ is a surjection, where $g(x) = 5x + 3$ for all $x \in \mathbb{R}$. Determine whether or not the following functions are surjections.

1. $k : A \to B$, where $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, and $k(a) = 4$, $k(b) = 1$, and $k(c) = 3$.
2. $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 3x + 2$ for all $x \in \mathbb{R}$.
3. $F : \mathbb{Z} \to \mathbb{Z}$ defined by $F(m) = 3m + 2$ for all $m \in \mathbb{Z}$.
4. $s : \mathbb{Z}_5 \to \mathbb{Z}_5$ defined by $s(x) = x^3$ for all $x \in \mathbb{Z}_5$.

Answer

Add texts here. Do not delete this text first.

The Importance of the Domain and Codomain

The functions in the next two examples will illustrate why the domain and the codomain of a function are just as important as the rule defining the outputs of a function when we need to determine if the function is a surjection.

Example 6.12 (A Function that Is Neither an Injection nor a Surjection)

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 + 1$. Notice that

$$f(2) = 5 \text{ and } f(-2) = 5.$$

This is enough to prove that the function f is not an injection since this shows that there exist two different inputs that produce the same output.

Since $f(x) = x^2 + 1$, we know that $f(x) \ge 1$ for all $x \in \mathbb{R}$. This implies that the function f is not a surjection. For example, -2 is in the codomain of f and $f(x) \ne -2$ for all x in the domain of f.

Example 6.13 (A Function that Is Not an Injection but Is a Surjection)

Let $T = \{y \in \mathbb{R} \mid y \ge 1\}$, and define $F : \mathbb{R} \to T$ by $F(x) = x^2 + 1$. As in Example 6.12, the function F is not an injection since $F(2) = F(-2) = 5$.

Is the function F a surjection? That is, does F map $\mathbb{R}$ onto T? As in Example 6.12, we do know that $F(x) \ge 1$ for all $x \in \mathbb{R}$.

To see if it is a surjection, we must determine if it is true that for every $y \in T$, there exists an $x \in \mathbb{R}$ such that $F(x) = y$. So we choose $y \in T$. The goal is to determine if there exists an $x \in \mathbb{R}$ such that

$$\begin{aligned} F(x) &= y, \text{ or} \\ x^2 + 1 &= y. \end{aligned} \tag{6.3.2}$$

One way to proceed is to work backward and solve the last equation (if possible) for x. Doing so, we get

$x^2 = y - 1$

$x = \sqrt{y-1}$ or $x = -\sqrt{y-1}$.

Now, since $y \in T$, we know that $y \ge 1$ and hence that $y - 1 \ge 0$. This means that $\sqrt{y-1} \in \mathbb{R}$. Hence, if we use $x = \sqrt{y-1}$, then $x \in \mathbb{R}$, and

$$\begin{aligned} F(x) &= F(\sqrt{y-1}) \\ &= (\sqrt{y-1})^2 + 1 \\ &= (y-1) + 1 \\ &= y. \end{aligned} \tag{6.3.3}$$

This proves that F is a surjection since we have shown that for all $y \in T$, there exists an

$x \in \mathbb{R}$ such that $F(x) = y$. Notice that for each $y \in T$, this was a constructive proof of the existence of an $x \in \mathbb{R}$ such that $F(x) = y$.

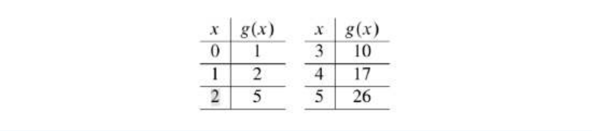
An Important Lesson.

In Examples 6.12 and 6.13, the same mathematical formula was used to determine the outputs for the functions. However, one function was not a surjection and the other one was a surjection. This illustrates the important fact that whether a function is surjective not only depends on the formula that defines the output of the function but also on the domain and codomain of the function.

The next example will show that whether or not a function is an injection also depends on the domain of the function.

Example 6.14 (A Function that Is a Injection but Is Not a Surjection)

Let $\mathbb{Z}^* = \{x \in \mathbb{Z} \mid x \geq 0\} = \mathbb{N} \cup \{0\}$. Define $g : \mathbb{Z}^* \to \mathbb{N}$ by $g(x) = x^2 + 1$. (Notice that this is the same formula used in Examples 6.12 and 6.13.) Following is a table of values for some inputs for the function g.



x	$g(x)$	x	$g(x)$
0	1	3	10
1	2	4	17
2	5	5	26

Notice that the codomain is $\mathbb{N}$, and the table of values suggests that some natural numbers are not outputs of this function. So it appears that the function g is not a surjection.

To prove that g is not a surjection, pick an element of $\mathbb{N}$ that does not appear to be in the range. We will use 3, and we will use a proof by contradiction to prove that there is no x in the domain ($\mathbb{Z}^*$) such that $g(x) = 3$. So we assume that there exists an $x \in \mathbb{Z}^*$ with $g(x) = 3$. Then

$$\begin{array}{rcl} x^2 + 1 &=& 3 \\ x^2 &=& 2 \\ x &=& \pm\sqrt{2}. \end{array} \tag{6.3.4}$$

But this is not possible since $\sqrt{2} \notin \mathbb{Z}^*$. Therefore, there is no $x \in \mathbb{Z}^*$ with $g(x) = 3$. This means that for every $x \in \mathbb{Z}^*$, $g(x) \neq 3$. Therefore, 3 is not in the range of g, and hence g is not a surjection.

The table of values suggests that different inputs produce different outputs, and hence that g is an injection. To prove that g is an injection, assume that $s, t \in \mathbb{Z}^*$ (the domain) with $g(s) = g(t)$. Then

$$\begin{array}{rcl} s^2 + 1 &=& t^2 + 1 \\ s^2 &=& t^2. \end{array} \tag{6.3.5}$$

Since $s, t \in \mathbb{Z}^*$, we know that $s \geq 0$ and $t \geq 0$. So the preceding equation implies that $s = t$. Hence, g is an injection.

An Important Lesson

The functions in the three preceding examples all used the same formula to determine the outputs. The functions in Exam- ples 6.12 and 6.13 are not injections but the function in Example 6.14 is an injection. This illustrates the important fact that whether a function is injective not only depends on the formula that defines the output of the function but also on the domain of the function.

Progress Check 6.15 (The Importance of the Domain and Codomain)

Let $R^+ = \{y \in \mathbb{R} \mid y > 0\}$. Define

\[\begin{array} {rcl} {f} &: & {\mathbb{R} \to \mathbb{R} \text{ by } f(x) = e^{-x}, \text{ for each } x \in \mathbb{R}, \text{ and }} \ {g} &: & {\mathbb{R} \to \mathbb{R}^{+} \text{ by } g(x) = e^{-x}, \text{ for each } x \in \mathbb{R}.}

Determine if each of these functions is an injection or a surjection. Justify your conclusions. **Note**: Before writing proofs, it might be helpful to draw the graph of $y = e^{-x}$. A reasonable graph can be obtained using $-3 \le x \le 3$ and $-2 \le y \le 10$. Please keep in mind that the graph is does not prove your conclusions, but may help you arrive at the correct conclusions, which will still need proof.

Answer

Add texts here. Do not delete this text first.

Working with a Function of Two Variables

It takes time and practice to become efficient at working with the formal definitions of injection and surjection. As we have seen, all parts of a function are important (the domain, the codomain, and the rule for determining outputs). This is especially true for functions of two variables.

For example, we define $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ by

$$f(a,b) = (2a+b, a-b) \text{ for all } (a,b) \in \mathbb{R} \times \mathbb{R}.$$

Notice that both the domain and the codomain of this function is the set $\mathbb{R} \times \mathbb{R}$. Thus, the inputs and the outputs of this function are ordered pairs of real numbers. For example,

$$f(1,1) = (3,0) \text{ and } f(-1,2) = (0,-3).$$

To explore wheter or not f is an injection, we assume that $(a,b) \in \mathbb{R} \times \mathbb{R}$, $(c,d) \in \mathbb{R} \times \mathbb{R}$, and $f(a,b) = f(c,d)$. This means that

$$(2a+b, a-b) = (2c+d, c-d).$$

Since this equation is an equality of ordered pairs, we see that

$$\begin{aligned} 2a+b &= 2c+d, \text{ and} \\ a-b &= c-d. \end{aligned} \tag{6.3.6}$$

By adding the corresponding sides of the two equations in this system, we obtain $3a = 3c$ and hence, $a = c$. Substituting $a = c$ into either equation in the system give us $b = d$. Since $a = c$ and $b = d$, we conclude that

$$(a,b) = (c,d).$$

Hence, we have shown that if $f(a,b) = f(c,d)$, then $(a,b) = (c,d)$. Therefore, f is an injection.

Now, to determine if f is a surjection, we let $(r,s) \in \mathbb{R} \times \mathbb{R}$, where (r,s) is considered to be an arbitrary element of the codomain of the function f . Can we find an ordered pair $(a,b) \in \mathbb{R} \times \mathbb{R}$ such that $f(a,b) = (r,s)$? Working backward, we see that in order to do this, we need

$$(2a+b, a-b) = (r,s).$$

That is, we need

$$2a+b = r \text{ and } a-b = s.$$

Solving this system for a and b yields

$$a = \frac{r+s}{3} \text{ and } b = \frac{r-2s}{3}.$$

Since $r, s \in \mathbb{R}$, we can conclude that $a \in \mathbb{R}$ and $b \in \mathbb{R}$ and hence that $(a,b) \in \mathbb{R} \times \mathbb{R}$.

We now need to verify that for. these values of a and b, we get $f(a,b) = (r,s)$. So

$$\begin{aligned} f(a,b) &= f(\frac{r+s}{3}, \frac{r-2s}{3}) \\ &= (2(\frac{r+s}{3}) + \frac{r-2s}{3}, \frac{r+s}{3} - \frac{r-2s}{3}) \\ &= (\frac{2r+2s+r-2s}{3}, \frac{r+s-r+2s}{3}) \\ &= (r,s). \end{aligned} \tag{6.3.7}$$

This proves that for all $(r, s) \in \mathbb{R} \times \mathbb{R}$, there exists $(a, b) \in \mathbb{R} \times \mathbb{R}$ such that $f(a, b) = (r, s)$. Hence, the function f is a surjection. Since f is both an injection and a surjection, it is a bijection.

Progress Check 6.16 (A Function of Two Variables)

Let $g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be defined by $g(x, y) = 2x + y$, for all $(x, y) \in \mathbb{R} \times \mathbb{R}$.

Note: Be careful! One major difference between this function and the previous example is that for the function g, the codomain is $\mathbb{R}$, not $\mathbb{R} \times \mathbb{R}$. It is a good idea to begin by computing several outputs for several inputs (and remember that the inputs are ordered pairs).

1. Notice that the ordered pair $(1, 0) \in \mathbb{R} \times \mathbb{R}$. That is (1, 0) is in the domain of g. Also notice that $g(1, 0) = 2$. Is it possible to find another ordered pair $(a, b) \in \mathbb{R} \times \mathbb{R}$ such that $g(a, b) = 2$?
2. Let $z \in \mathbb{R}$. Then $(0, z) \in \mathbb{R} \times \mathbb{R}$ and so $(0, z) \in \mathrm{dom}(g)$. Now determine $g(0, z)$?
3. Is the function g an injection? Is the function g a surjection? Justify your conclusions.

Answer

Add texts here. Do not delete this text first.

Exercise 6.3

1. (a) Draw an arrow diagram that represents a function that is an injection but is not a surjection.
   (b) Draw an arrow diagram that represents a function that is an injection and is a surjection.
   (c) Draw an arrow diagram that represents a function that is not an injection and is not a surjection.
   (d) Draw an arrow diagram that represents a function that is not an injection but is a surjection.
   (e) Draw an arrow diagram that represents a function that is not a bijection.
2. Let $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ and let $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. For each of the following functions, determine if the function is an injection and determine if the function is a surjection. Justify all conclusions.

   (a) $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $f(x) = x^2 + 4$ (mod 5), for all $x \in \mathbb{Z}_5$
   (b) $g : \mathbb{Z}_6 \to \mathbb{Z}_6$ by $g(x) = x^2 + 4$ (mod 6), for all $x \in \mathbb{Z}_6$
   (c) $F : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $F(x) = x^3 + 4$ (mod 5), for all $x \in \mathbb{Z}_5$
3. For each of the following functions, determine if the function is an injection and determine if the function is a surjection. Justify all conclusions.

   (a) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 3x + 1$, for all $x \in \mathbb{Z}$.
   (b) $F : \mathbb{Q} \to \mathbb{Q}$ defined by $F(x) = 3x + 1$, for all $x \in \mathbb{Q}$.
   (c) $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^3$, for all $x \in \mathbb{R}$.
   (d) $G : \mathbb{Q} \to \mathbb{Q}$ defined by $G(x) = x^3$, for all $x \in \mathbb{Q}$.
   (e) $k : \mathbb{R} \to \mathbb{R}$ defined by $k(x) = e^{-x^2}$, for all $x \in \mathbb{R}$.
   (f) $K : \mathbb{R}^* \to \mathbb{R}$ defined by $K(x) = e^{-x^2}$, for all $x \in \mathbb{R}^*$.
   Note: $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \geq 0\}$.
   (g) $K_1 : \mathbb{R}^* \to T$ defined by $K_1(x) = e^{-x^2}$, for all $x \in \mathbb{R}^*$, where $T = \{y \in \mathbb{R} \mid 0 < y \leq 1\}$.
   (h) $h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = \dfrac{2x}{x^2 + 4}$, for all $x \in \mathbb{R}$.
   (i) $H : \{x \in \mathbb{R} \mid x \geq 0\} \to \{y \in \mathbb{R} \mid 0 \leq y \leq \frac{1}{2}\}$ defined by $H(x) = \dfrac{2x}{x^2 + 4}$, for all $x \in \{x \in \mathbb{R} \mid x \geq 0\}$.
4. For each of the following functions, determine if the function is a bijection. Justify all conclusions.

   (a) $F : \mathbb{R} \to \mathbb{R}$ defined by $F(x) = 5x + 3$, for all $x \in \mathbb{R}$.
   (b) $G : \mathbb{Z} \to \mathbb{Z}$ defined by $G(x) = 5x + 3$, for all $x \in \mathbb{Z}$.
   (c) $f : (\mathbb{R} - \{4\}) \to \mathbb{R}$ defined by $f(x) = \dfrac{3x}{x - 4}$, for all $x \in (\mathbb{R} - \{4\})$.
   (d) $g : (\mathbb{R} - \{4\}) \to (\mathbb{R} - \{3\})$ defined by $g(x) = \dfrac{3x}{x - 4}$, for all $x \in (\mathbb{R} - \{4\})$.

5. Let $s : \mathbb{N} \to \mathbb{N}$, where for each $n \in \mathbb{N}$, $s(n)$ is the sum of the distinct natural number divisors of n. This is the **sum of the divisors function** that was introduced in Preview Activity $6.3.2$ from Section 6.1. Is s an injection? Is s a surjection? Justify your conclusions.
6. Let $d : \mathbb{N} \to \mathbb{N}$, where $d(n)$ is the number of natural number divisors of n. This is the **number of divisors function** introduced in Exercise (6) from Section 6.1. Is the function d an injection? Is the function d a surjection? Justify your conclusions.
7. In Preview Activity $6.3.2$ from Section 6.1 , we introduced the **birthday function**. Is the birthday function an injection? Is it a surjection? Justify your conclusions.
8. (a) Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be defined by $f(m, n) = 2m + n$. Is the function f an injection? Is the function f a surjection? Justify your conclusions.
   (b) Let $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be defined by $g(m, n) = 6m + 3n$. Is the function g an injection? Is the function g a surjection? Justify your conclusions.
9. (a) Let $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ be defined by $f(x, y) = (2x, x + y)$. Is the function f an injection? Is the function f a surjection? Justify your conclusions.
   (b) Let $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be defined by $g(x, y) = (2x, x + y)$. Is the function g an injection? Is the function g a surjection? Justify your conclusions.
10. Let $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be the function defined by $f(x, y) = -x^2y + 3y$, for all $(x, y) \in \mathbb{R} \times \mathbb{R}$. Is the function f and injection? Is the function f a surjection? Justify your conclusions.
11. Let $g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be the function defined by $g(x, y) = (x^3 + 2) siny$, for all $(x, y) \in \mathbb{R} \times \mathbb{R}$. Is the function g and injection? Is the function g a surjection? Justify your conclusions.
12. Let A be a nonempty set. The **identity function on the set** A, denoted by I_A, is the function $I_A : A \to A$ defined by $I_A(x) = x$ for every x in A. Is I_A an injection? Is I_A a surjection? Justify your conclusions.
13. Let A and B be two nonempty sets. Define

$$p_1 : A \times B \to A \text{ by } p_1(a, b) = a \tag{6.3.8}$$

    for every $(a, b) \in A \times B$. That is the **first projection function** introduced in Exercise (5) in Section 6.2.
    (a) Is the function p_1 a surjection? Justify your conclusion.
    (b) If $B = \{b\}$, is the function p_1 an injection? Justify your conclusion.
    (c) Under what condition(s) is the function p_1 not an injection? Make a conjecture and prove it.
14. Define $f : \mathbb{N} \to \mathbb{Z}$ be defined as follows: For each $n \in \mathbb{N}$,

$$f(n) = \frac{1 + (-1)^n(2n - 1)}{4}. \tag{6.3.9}$$

    Is the function f an injection? Is the function f a surjection? Justify your conclusions.

    Suggestions. Start by calculating several outputs for the function before you attempt to write a proof. In exploring whether or not the function is an injection, it might be a good idea to uses cases based on whether the inputs are even or odd. In exploring whether f is a surjection, consider using cases based on whether the output is positive or less than or equal to zero.
15. Let C be the set of all real functions that are continuous on the closed interval [0, 1]. Define the function $A : C \to \mathbb{R}$ as follows: For each $f \in C$.

$$A(f) = \int_0^1 f(x) dx. \tag{6.3.10}$$

    Is the function A an injection? Is it a surjection? Justify your conclusions.
16. Let $A = \{(m, n) \mid m \in \mathbb{Z}, n \in \mathbb{Z}, \text{ and } n \neq 0\}$. Define $f : A \to \mathbb{Q}$ as follows:
    For each $(m, n) \in A$, $f(m, n) = \dfrac{m + n}{n}$.
    (a) Is the function f an injection? Justify your conclusion.
    (b) Is the function f a surjection? Justify your conclusion.

17. **Evaluation of proofs**
See the instructions for Exercise (19) on page 100 from Section 3.1.

✎ (a)

Proposition. The function $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ defined by $f(x, y) = (2x + y, x - y)$ is an injection.

Proof

For each (a, b) and (c, d) in $\mathbb{R} \times \mathbb{R}$, if $f(a, b) = f(c, d)$, then

$$(2a + b, a - b) = (2c + d, c - d).$$

We will use systems of equations to prove that $a = c$ and $b = d$.

$$\begin{array}{rcl} 2a + b &=& 2c + d \\ a - b &=& c - d \\ 3a &=& 3c \\ a &=& c \end{array} \tag{6.3.11}$$

Since $a = c$, we see that

$$(2c + b, c - b) = (2c + d, c - d).$$

So $b = d$. Therefore, we have proved that the function f is an injection.

✎ (b)

Proposition. The function $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ defined by $f(x, y) = (2x + y, x - y)$ is an surjection.

Proof

We need to find an ordered pair such that $f(x, y) = (a, b)$ for each (a, b) in $\mathbb{R} \times \mathbb{R}$. That is, we need $(2x + y, x - y) = (a, b)$, or

$$2x + y = a \text{ and } x - y = b.$$

Treating these two equations as a system of equations and solving for x and y, we find that

$$x = \frac{a + b}{3} \text{ and } y = \frac{a - 2b}{3}.$$

Hence, x and y are real numbers, $(x, y) \in \mathbb{R} \times \mathbb{R}$, and

$$\begin{array}{rcl} f(x, y) &=& f(\frac{a + b}{3}, \frac{a - 2b}{3}) \\ &=& (2(\frac{a + b}{3}) + \frac{a - 2b}{3}, \frac{a + b}{3} - \frac{a - 2b}{3}) \\ &=& (\frac{2a + 2b + a - 2b}{3}, \frac{a + b - a + 2b}{3}) \\ &=& (\frac{3a}{3}, \frac{3b}{3}) \\ &=& (a, b). \end{array} \tag{6.3.12}$$

Therefore, we. have proved that for every $(a, b) \in \mathbb{R} \times \mathbb{R}$, there exists an $(x, y) \in \mathbb{R} \times \mathbb{R}$ such that $f(x, y) = (a, b)$. This proves that the function f is a surjection.

Explorations and Activities

18. **Piecewise Defined Functions**. We often say that a function is a **piecewise defined function** if it has different rules for determining the output for different parts of its domain. For example, we can define a function $f : \mathbb{R} \to \mathbb{R}$ by giving a rule for calculating $f(x)$ when $x \geq 0$ and giving a rule for calculating $f(x)$ when x < 0 as follows:

$$f(x) = \begin{cases} x^2 + 1, & \text{if } x \geq 0; \\ x - 1 & \text{if } x < 0. \end{cases} \tag{6.3.13}$$

(a) Sketch a graph of the function f. Is the function f and injection? Is the function f a surjection? Justify your conclusions.

For each of the following functions, determine if the function is an injection and determine if the function is a surjection. Justify all conclusions.

(b) $g : [0, 1] \to (0, 1)$ by

$$g(x) = \begin{cases} 0.8, & \text{if } x = 0; \\ 0.5x & \text{if } 0 < x < 1; \\ 0.6 & \text{if } x = 1. \end{cases} \tag{6.3.14}$$

(c) $h : \mathbb{Z} \to \{0, 1\}$ by

$$h(x) = \begin{cases} 0, & \text{if } x \text{ is even;} \\ 1, & \text{if } x \text{ is odd.} \end{cases} \tag{6.3.15}$$

19. **Functions Whose Domain is** $\mathcal{M}_2(\mathbb{R})$. Let $\mathcal{M}_2(\mathbb{R})$. represent the set of all 2 by 2 matrices over $\mathbb{R}$.

(a) Defien det: $\mathcal{M}_2(\mathbb{R}) \to \mathbb{R}$ by

$$det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc. \tag{6.3.16}$$

This is the **determinant function** introduced in Exercise (9) from Section 6.2. Is the determinant function an injection? Is the determinant function a surjection? Justify your conclusions.

(b) Define tran: $\mathcal{M}_2(\mathbb{R}) \to \mathcal{M}_2(\mathbb{R})$ by

$$tran \begin{bmatrix} a & b \\ c & d \end{bmatrix} = A^T = \begin{bmatrix} a & c \\ b & d \end{bmatrix}. \tag{6.3.17}$$

This is the **transpose function** introduced in Exercise (10) from Section 6.2. Is the transpose function an injection? Is the transpose function a surjection? Justify your conclusions.

(c) Define $F : \mathcal{M}_2(\mathbb{R}) \to \mathbb{R}$ by

$$F \begin{bmatrix} a & b \\ c & d \end{bmatrix} = a^2 + d^2 - b^2 - c^2. \tag{6.3.18}$$

Is the function F an injection? Is the function F a surjection? Justify your conclusions.

Answer

Add texts here. Do not delete this text first.

This page titled 6.3: Injections, Surjections, and Bijections is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

6.4: Composition of Functions

? PREVIEW ACTIVITY 6.4.1: Constructing a New Function

Let $A = \{a, b, c, d\}$, $B = \{p, q, r\}$, and $C = \{s, t, u, v\}$. The arrow diagram in Figure 6.6 shows two functions: $f : A \to B$ and $g : B \to C$. Notice that if $x \in A$, then $f(x) \in B$. Since $f(x) \in B$, we can apply the function g to $f(x)$, and we obtain $g(f(x))$, which is an element of C.

Using this process, determine $g(f(a))$, $g(f(b))$, $g(f(c))$, and $g(f(d))$. Then explain how we can use this information to define a function from A to C.

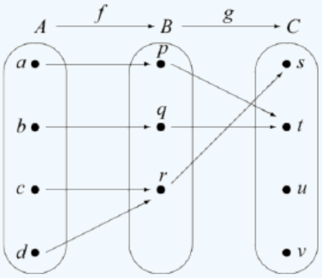


Figure 6.6: Arrow Diagram Showing Two Functions

? PREVIEW ACTIVITY 6.4.1: Verbal Descriptions of Functions

The outputs of most real functions we have studied in previous mathematics courses have been determined by mathematical expressions. In many cases, it is possible to use these expressions to give step-by-step verbal descriptions of how to compute the outputs. For example, if

$$f : \mathbb{R} \to \mathbb{R} \text{ is defined by } f(x) = (3x+2)^3,$$

we could describe how to compute the outputs as follows:

Step	**Verbal Description**	**Symbolic Result**
1	Choose an input.	x
2	Multiply by 3.	$3x$
3	Add 2.	$3x+2$
4	Cube the result.	$(3x+3)^3$

Complete step-by-step verbal descriptions for each of the following functions.

1. $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = \sqrt{3x^2+2}$, for each $x \in \mathbb{R}$.
2. $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = \sin(3x^2+2)$, for each $x \in \mathbb{R}$.
3. $h : \mathbb{R} \to \mathbb{R}$ by $h(x) = e^{3x^2+2}$, for each $x \in \mathbb{R}$.
4. $G : \mathbb{R} \to \mathbb{R}$ by $G(x) = \ln(x^4+3)$, for each $x \in \mathbb{R}$.
5. $k : \mathbb{R} \to \mathbb{R}$ by $k(x) = \sqrt[3]{\dfrac{\sin(4x+3)}{x^2+1}}$, for each $x \in \mathbb{R}$.

Composition of Functions

There are several ways to combine two existing functions to create a new function. For example, in calculus, we learned how to form the product and quotient of two functions and then how to use the product rule to determine the derivative of a product of two functions and the quotient rule to determine the derivative of the quotient of two functions. The chain rule in calculus was used to determine the derivative of the composition of two functions, and in this section, we will focus only on the composition of two functions. We will then consider some results about the compositions of injections and surjections.

The basic idea of function composition is that when possible, the output of a function f is used as the input of a function g. This can be referred to as “f followed by g” and is called the composition of f and g. In previous mathematics courses, we used this idea to determine a formula for the composition of two real functions.

For example, if

$$f(x) = 3x^2 + 2 \text{ and } g(x) = sin x$$

then we can compute $g(f(x))$ as follows:

$$\begin{aligned} g(f(x)) &= g(3x^2 + 2) \\ &= sin(3x^2 + 2). \end{aligned} \tag{6.4.1}$$

In this case, $f(x)$, the output of the function f, was used as the input for the function g. We now give the formal definition of the composition of two functions.

Definition: composite function

Let A, B, and C be nonempty sets, and let $f : A \to B$ and $g : B \to C$ be functions. The *composition* of f and g is the function $g \circ f : A \to C$ defined by

$$(g \circ f)(x) = g(f(x))$$

for all $x \in A$. We often refer to the function $g \circ f$ as a *composite function*.

It is helpful to think of composite function $g \circ f$ as "f **followed by** g". We then refer to f as the **inner function** and g as the **outer function**.

Composition and Arrow Diagrams

The concept of the composition of two functions can be illustrated with arrow diagrams when the domain and codomain of the functions are small, finite sets. Although the term “composition” was not used then, this was done in Preview Activity $6.4.1$, and another example is given here.

Let $A = \{a, b, c, d\}$, $B = \{p, q, r\}$, and $C = \{s, t, u, v\}$. The arrow diagram in Figure 6.7 shows two functions: $f : A \to B$ and $g : B \to C$.

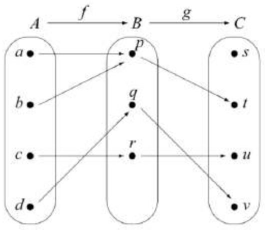


Figure 6.7: Arrow Diagram for Two Functions

If we follow the arrows from the set A to the set C, we will use the outputs of f as inputs of g, and get the arrow diagram from A to C shown in Figure 6.8. This diagram represents the composition of f followed by g.

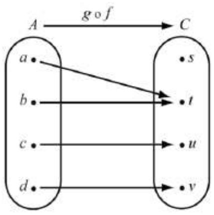


Figure 6.8: Arrow Diagram for $g \circ f : A \to C$

Progress Check 6.17 (The Composition of Two Functions)

Let $A = \{a, b, c, d\}$ and $B = \{1, 2, 3\}$. Define the function f and g as follows:

$f : A \to B$ defined by $f(a) = 2$, $f(b) = 3$, $f(c) = 1$, and $f(d) = 2$.

$g : A \to B$ defined by $g(1) = 3$. $g(2) = 1$, and $g(3) = 2$.

Create arrow diagrams for the function f, g, $g \circ f$, and $g \circ g$.

Answer

Add texts here. Do not delete this text first.

Decomposing Functions

We use the chain rule in calculus to find the derivative of a composite function. The first step in the process is to recognize a given function as a composite function. This can be done in many ways, but the work in Preview Activity $6.4.2$ can be used to decompose a function in a way that works well with the chain rule. The use of the terms “inner function” and “outer function” can also be helpful. The idea is that we use the last step in the process to represent the outer function, and the steps prior to that to represent the inner function. So for the function,

$$f : \mathbb{R} \to \mathbb{R} \text{ by } f(x) = (3x + 2)^3,$$

the last step in the verbal description table was to cube the result. This means that we will use the function g (the cubing function) as the outer function and will use the prior steps as the inner function. We will denote the inner function by h. So we let $h : \mathbb{R} \to \mathbb{R}$ by $h(x) = 3x + 2$ and $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^3$. Then

$$\begin{aligned}(g \circ h)(x) &= g(h(x)) \\ &= g(3x + 2) \\ &= (3x + 2)^3 \\ &= f(x).\end{aligned} \tag{6.4.2}$$

We see that $g \circ h = f$ and, hence, we have “decomposed” the function f. It should be noted that there are other ways to write the function f as a composition of two functions, but the way just described is the one that works well with the chain rule. In this case, the chain rule gives

$$\begin{aligned}f'(x) &= (g \circ h)'(x) \\ &= g'(h(x))h'(x) \\ &= 3(h(x))^2 \cdot 3 \\ &= g(3x + 2)^2\end{aligned} \tag{6.4.3}$$

Progress Check 6.18 (Decomposing Functions

Write each of the following functions as the composition of two functions.

1. $F : \mathbb{R} \to \mathbb{R}$ by $F(x) = (x^2 + 3)^3$
2. $G : \mathbb{R} \to \mathbb{R}$ by $G(x) = In(x^2 + 3)$
3. $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x) = |x^2 - 3|$
4. $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = cos(\dfrac{2x - 3}{x^2 + 1})$

Answer

Add texts here. Do not delete this text first.

Theorems about Composite Functions

If $f : A \to B$ and $g : B \to C$, then we can form the composite function $g \circ f : A \to C$. In Section 6.3, we learned about injections and surjections. We now explore what type of function $g \circ f$ will be if the functions f and g are injections (or surjections).

? Progress Check 6.19: Compositions of Injections and Surjections

Although other representations of functions can be used, it will be helpful to use arrow diagrams to represent the functions in this progress check. We will use the following sets:

$$A = \{a, b, c\},\ B = \{p, q, r\},\ C = \{u, v, w, x\}, \text{ and } D = \{u, v\}.$$

1. Draw an arrow diagram for a function $f : A \to B$ that is an injection and an arrow diagram for a function $g : B \to C$ that is an injection. In this case, is the composite function $g \circ f : A \to C$ an injection? Explain.
2. Draw an arrow diagram for a function $f : A \to B$ that is a surjection and an arrow diagram for a function $g : B \to D$ that is a surjection. In this case, is the composite function $g \circ f : A \to D$ a surjection? Explain.
3. Draw an arrow diagram for a function $f : A \to B$ that is a bijection and an arrow diagram for a function $g : B \to A$ that is a bijection. In this case, is the composite function $g \circ f : A \to A$ bijection? Explain.

Answer

Add texts here. Do not delete this text first.

In Progress Check 6.19, we explored some properties of composite functions related to injections, surjections, and bijections. The following theorem contains results that these explorations were intended to illustrate. Some of the proofs will be included in the exercises.

Theorem 6.20.

Let A, B, and C be nonempty sets and assume that $f : A \to B$ and $g : B \to C$.

1. If f and g are both injections, then $(g \circ f) : A \to C$ is an injection.
2. If f and g are both surjections, then $(g \circ f) : A \to C$ is an surjection.
3. If f and g are both bijections, then $(g \circ f) : A \to C$ is an bijection.

Proof

The proof of Part (1) is Exercise (6).

Part (3) is a direct consequence of the first two parts. We will discuss a process for constructing a proof of Part (2). Using the forward-backward process, we first look at the conclusion of the conditional statement in Part (2). The goal is to prove that $g \circ f$ is a surjection. Since $(g \circ f) : A \to C$, this is equivalent to proving that

$$\text{For all } c \in C, \text{ there exists an } a \in A \text{ such that } (g \circ f)(a) = c.$$

Since this statement in the backward process uses a universal quantifier, we will use the choose-an-element method and choose an arbitrary element c in the set C. The goal now is to find an $a \in A$ such that $(g \circ f)(a) = c$.

Now we can look at the hypotheses. In particular, we are assuming that both $f : A \to B$ and $g : B \to C$ are surjections. Since we have chosen $c \in C$, and $g : B \to C$ is a surjection, we know that

$$\text{there exists a } b \in B \text{ such that } g(b) = c.$$

Now, $b \in B$ and $f : A \to B$ is a surjection. Hence

$$\text{there exists an } a \in A \text{ such that } f(a) = b.$$

If we now compute $(g \circ f)(a)$, we will see that

$$(g \circ f)(a) = g(f(a)) = g(b) = c.$$

We can now write the proof as follows:

Proof of Theorem 6.20, Part (2)

Let A, B, and C be nonempty sets and assume that $f : A \to B$ and $g : B \to C$ are both surjections. We will prove that $g \circ f : A \to C$ is a surjection.

Let c be an arbitrary element of C. We will prove there exists an $a \in A$ such that $(g \circ f)(a) = c$. Since $g : B \to C$ is a surjection, we conclude that

$$\text{there exists a } b \in B \text{ such that } g(b) = c.$$

Now, $b \in B$ and $f : A \to B$ is a surjection. Hence

$$\text{there exists an } a \in A \text{ such that } f(a) = b.$$

We now see that

$$\begin{aligned}(g \circ f)(a) &= g(f(a)) \\ &= g(b) \\ &= c.\end{aligned}$$

We have now shown that for every $c \in C$, there exists an $a \in A$ such that $(g \circ f)(a) = c$, and this proves that $g \circ f$ is a surjection.

Theorem 6.20 shows us that if f and g are both special types of functions, then the composition of f followed by g is also that type of function.The next question is, “If the composition of f followed by g is an injection (or surjection), can we make any conclusions about f or g?” A partial answer to this question is provided in Theorem 6.21. This theorem will be investigated and proved in the Explorations and Activities for this section. See Exercise (10).

Theorem 6.21

Let A, B, and C be nonempty sets and assume that $f : A \to B$ and $g : B \to C$.

1. If $g \circ f : A \to C$ is an injection, then $f : A \to B$ is an injection.
2. If $g \circ f : A \to C$ is a surjection, then $f : A \to B$ is a surjection.

Exercise 6.4

1. In our definition of the composition of two functions, f and g, we required that the domain of g be equal to the codomain of f. However, it is sometimes possible to form the composite function $g \circ f$ even though dom(g) $\ne$ codom(f). For example, let

$$\begin{array}{lll} f : \mathbb{R} \to \mathbb{R} & textbedefinedby & f(x) = x^2 + 1, \text{ and let} \\ g : \mathbb{R} - \{0\} \to \mathbb{R} & textbedefinedby & g(x) = \dfrac{1}{x}. \end{array} \tag{6.4.4}$$

   (a) Is it possible to determine $(g \circ f)(x)$ for all $x \in \mathbb{R}$? Explain.
   (b) In general, let $f : A \to T$ and $g : B \to C$. Find a condition on the domain of g (other than $B = T$) that results in a meaningful definition of the composite function $g \circ f : A \to C$.
2. Let $h : \mathbb{R} \to \mathbb{R}$ be defined $h(x) = 3x + 2$ and $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^3$. Determine formulas for the composite functions $g \circ h$ and $h \circ g$. Is the function $g \circ h$ equal to the function $h \circ g$? Explain. What does this tell you about the operation of composition of functions?
3. Following are formulas for certain real functions. Write each of these real functions as the composition of two functions. That is, decompose each of the functions.

   (a) $F(x) = cos(e^x)$
   (b) $G(x) = e^{cos(x)}$
   (c) $H(x) = \dfrac{1}{sin x}$
   (d) $K(x) = cos(e^{-x^2})$

CC BY-NC-SA

4. The identity function on a set S, denoted by I_S, is defined as follows: $I_S : S \to S$ by $I_s(x) = x$ for each $x \in S$. Let $f : A \to B$.

   (a) For each $x \in A$, determine $(f \circ I_A)(x)$ and use this to prove that $f \circ I_A = f$.
   (b) Prove that $I_B \circ f = f$.
5. (a) Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$, let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = sin x$, and let $h : \mathbb{R} \to \mathbb{R}$ be defined by $h(x) = \sqrt[3]{x}$.

   Determine formulas for $[(h \circ g) \circ f](x)$ and $[h \circ (g \circ f)](x)$.

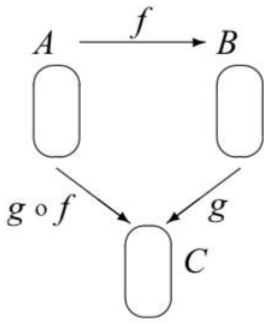
   Does this prove that $(h \circ g) \circ f = h \circ (g \circ f)$ for these particular functions? Explain.

   (b) Now let A, B, and C be sets and let $f : A \to B$, $g : B \to C$, and $h : C \to D$. Prove that $(h \circ g) \circ f = h \circ (g \circ f)$. That is, prove that function composition is an associative operation.
6. Prove Part (1) of Theorem 6.20.
   Let A, B, and C be nonempty sets and let $f : A \to B$ and $g : B \to C$. If f and g are both injections, then $g \circ f$ is an injection.
7. For each of the following, give an example of functions $f : A \to B$ and $g : B \to C$ that satisfy the stated conditions, or explain why no such example exists.

   (a) The function f is a surjection, but the function $g \circ f$ is not a surjection.
   (b) The function f is an injection, but the function $g \circ f$ is not an injection.
   (c) The function g is a surjection, but the function $g \circ f$ is not a surjection.
   (d) The function g is an injection, but the function $g \circ f$ is not an injection.
   (e) The function f is not a surjection, but the function $g \circ f$ is a surjection.
   (f) The function f is not an injection, but the function $g \circ f$ is an injection.
   (g) The function f is not an injection, but the function $g \circ f$ is an injection.
   (h) The function g is not an injection, but the function $g \circ f$ is an injection.
8. Let A be a nonempty set and let $f : A \to A$. For each $n \in \mathbb{N}$, define a funciton $f^n : A \to A$ recursively as follows: $f^1 = f$ and for each $n \in \mathbb{N}$, $f^{n+1} = f \circ f^n$. For example, $f^2 = f \circ f^1 = f \circ f$ and $f^3 = f \circ f^2 = f \circ (f \circ f)$.

   (a) Let $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x + 1$ for each $x \in \mathbb{R}$. For each $n \in \mathbb{N}$ and for each $x \in \mathbb{R}$, determine a formula for $f^n(x)$ and use induction to prove that your formula is correct.
   (b) Let $a, b \in \mathbb{R}$ and let $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = ax + b$ for each $x \in \mathbb{R}$. For each $n \in \mathbb{N}$ and for each $x \in \mathbb{R}$, determine a formula for $f^n(x)$ and use induction to prove that your formula is correct.
   (c) Now let A be a nonempty set and let $f : A \to A$. Use induction to prove that for each $n \in \mathbb{N}$, $f^{n+1} = f^n \circ f$. (**Note:** You will need to use the result in Exercise (5).)

   Explorations and Activities
9. **Exploring Composite Functions**. Let A, B, and C be nonempty sets and let $f : A \to B$ and $g : B \to C$. For this activity, it may be useful to draw your arrow diagrams in a triangular arrangement as follows:



It might be helpful to consider examples where the sets are small. Try constructing examples where the set A has 2 elements, the set B has 3 elements, and the set C has 2 elements.

(a) Is it possible to construct an example where $g \circ f$ is an injection, f is an injection, but g is not an injection? Either construct such an example or explain why it is not possible.
(b) Is it possible to construct an example where $g \circ f$ is an injection, g is an injection, but f is not an injection? Either construct such an example or explain why it is not possible.
(c) Is it possible to construct an example where $g \circ f$ is a surjection, f is a surjection, but g is not a surjection? Either construct such an example or explain why it is not possible.
(d) Is it possible to construct an example where $g \circ f$ is a surjection, g is a surjection, but f is not a surjection? Either construct such an example or explain why it is not possible.

10. The Proof of Theorem 6.21. Use the ideas from Exercise (9) to prove Theorem 6.21. Let A, B and C be nonempty sets and let $f : A \to B$ and $g : B \to C$.

    (a) If $g \circ f : A \to C$ is an injection, then $f : A \to B$ is an injection.
    (b) If $g \circ f : A \to C$ is a surjection, then $g : B \to C$ is a surjection.

    Hint: For part (a), start by asking, “What do we have to do to prove that f is an injection? ” Start with a similar question for part (b).

Answer

Add texts here. Do not delete this text first.

This page titled 6.4: Composition of Functions is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

6.5: Inverse Functions

For this section, we will use the concept of Cartesian product of two sets A and B, denoted by $A \times B$, which is the set of all ordered pairs (x, y) where $x \in A$ and $y \in B$. That is,

$$A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}.$$

See Preview Activity $6.5.2$ in Section 5.4 for a more thorough discussion of this concept.

? PREVIEW ACTIVITY $6.5.1$: Functions and Sets of Ordered Pairs

When we graph a real function, we plot ordered pairs in the Cartesian plane where the first coordinate is the input of the function and the second coordinate is the output of the function. For example, if $g : \mathbb{R} \to \mathbb{R}$, then every point on the graph of g is an ordered pair (x, y) of real numbers where $y = g(x)$. This shows how we can generate ordered pairs from a function. It happens that we can do this with any function. For example, let

$$A = \{1, 2, 3\} \text{ and } B = \{a, b\}.$$

Define the function $F : A \to B$ by

$$F(1) = a,\ F(2) = b, \text{ and } F(3) = b.$$

We can convert each of these to an ordered pair in $A \times B$ by using the input as the first coordinate and the output as the second coordinate. For example, $F(1) = a$ is converted to $(1, a)$, $F(2) = b$ is converted to $(2, b)$, and $F(3) = b$ is converted to $(3, b)$. So we can think of this function as a set of ordered pairs, which is a subset of $A \times B$, and write

$$F = \{(1, a), (2, b), (3, b)\}.$$

Note: Since F is the name of the function, it is customary to use F as the name for the set of ordered pairs.

1. Let $A = \{1, 2, 3\}$ and let $C = \{a, b, c, d\}$. Define the function $g : A \to C$ by $g(1) = a$, $g(2) = b$, and $g(3) = d$. Write the function g as a set of ordered pairs in $A \times C$.

For another example, if we have a real function, such as: $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^2 - 2$, then we can think of g as the following infinite subset of $\mathbb{R} \times \mathbb{R}$:

$$g = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2 - 2\}.$$

We can also write this sometimes write this as $g = \{(x, x^2 - 2) \mid x \in \mathbb{R}\}$.

2. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(m) = 3m + 5$, for all $m \in \mathbb{Z}$. Use set builder notation to write the function f as a set of ordered pairs, and then use the roster method to write the function f as a set of ordered pairs.

So any function $f : A \to B$ can be thought of as a set of ordered pairs that is a subset of $A \times B$. This subset is

$$f = \{(a, f(a)) \mid a \in A\} \text{ or } f = \{(a, b) \in A \times B \mid b = f(a)\}.$$

On the other hand, if we started with $A = \{1, 2, 3\}$, $B = \{a, b\}$, and

$$G = \{(1, a), (2, a), (3, b)\} \subseteq A \times B,$$

then we could think of G as a function from A to B with $G(1) = a$, $G(2) = a$, and $G(3) = b$. The idea is to use the first coordinate of each ordered pair as the input, and the second coordinate as the output. However, not every subset of $A \times B$ can be used to define a function from A to B. This is explored in the following questions.

3. Let $f = \{(1, a), (2, a), (3, a), (1, b)\}$. Could this set of ordered pairs be used to define a function from A to B? Explain.
4. Let $g = \{(1, a), (2, a), (3, a)\}$. Could this set of ordered pairs be used to define a function from A to B? Explain.
5. Let $h = \{(1, a), (2, b)\}$. Could this set of ordered pairs be used to define a function from A to B? Explain.

? PREVIEW ACTIVITY $6.5.1$: A Composition of Two Specific Functions

Let $A = \{a, b, c, d\}$ and let $B = \{p, q, r, s\}$.

1. Construct an example of a function $f : A \to B$ that is a bijection. Draw an arrow diagram for this function.

2. On your arrow diagram, draw an arrow from each element of B back to its corresponding element in A. Explain why this defines a function from B to A.
3. If the name of the function in Part (2) is g, so that $g : B \to A$, what are $g(p)$, $g(q)$, $g(r)$, and $g(s)$?
4. Construct a table of values for each of the functions $g \circ f : A \to A$ and $f \circ g : B \to B$. What do you observe about these tables of values?

The Ordered Pair Representation of a Function

In Preview Activity 6.5.1, we observed that if we have a function $f : A \to B$, we can generate a set of ordered pairs f that is a subset of $A \times B$ as follows:

$$f = \{(a, f(a) \mid a \in A\} \text{ or } f = \{(a, b) \in A \times B \mid b = f(a)\}.$$

However, we also learned that some sets of ordered pairs cannot be used to define a function. We now wish to explore under what conditions a set of ordered pairs can be used to define a function. Starting with a function $f : A \to B$, since dom(f) = A, we know that

$$\text{For every } a \in A, \text{ there exists a } b \in B \text{ such that } (a, b) \in f. \tag{6.5.1}$$

Specifically, we use $b = f(a)$. This says that every element of A can be used as an input. In addition, to be a function, each input can produce only one output. In terms of ordered pairs, this means that there will never be two ordered pairs (a, b) and (a, c) in the function f where $a \in A$, $b, c \in B$, and $b \neq c$. We can formulate this as a conditional statement as follows:

$$\begin{gathered}\text{For every } a \in A \text{ and every } b, c \in B, \\ \text{if } (a, b) \in f \text{ and } (a, c) \in f, \text{ then } b = c.\end{gathered} \tag{6.5.2}$$

This also means that if we start with a subset f of $A \times B$ that satisfies conditions in Equation 6.5.1 and 6.5.2, then we can consider f to be a function from A to B by using $b = f(a)$ whenever (a, b) is in f. This proves the following theorem.

Theorem 6.22

Let A and B be nonempty sets and let f be a subset of $A \times B$ that satisfies the following two properties:

- For every $a \in A$, there exists $b \in B$ such that $(a, b) \in f$; and
- For every $a \in A$ and every $b, c \in B$, if $(a, b) \in f$ and $(a, c) \in f$, then $b = c$.

If we use $f(a) = b$ whenever $(a, b) \in f$, then f is a function from A to B.

A Note about Theorem 6.22. The first condition in Theorem 6.22 means that every element of A is an input, and the second condition ensures that every input has exactly one output. Many texts will use Theorem 6.22 as the definition of a function. Many mathematicians believe that this ordered pair representation of a function is the most rigorous definition of a function. It allows us to use set theory to work with and compare functions. For example, equality of functions becomes a question of equality of sets. Therefore, many textbooks will use the ordered pair representation of a function as the definition of a function.

? Progress Check 6.23 (Sets of Ordered Pairs that Are Not Functions)

Let $A = \{1, 2, 3\}$ and let $B = \{a, b\}$. Explain why each of the following subsets of $A \times B$ cannot be used to define a function from A to B.

1. $F = \{(1, a), (2, a)\}$,
2. $G = \{(1, a), (2, b), (3, c), (2, c)\}$.

Answer

Add texts here. Do not delete this text first.

The Inverse of a Function

In previous mathematics courses, we learned that the exponential function (with base e) and the natural logarithm functions are inverses of each other. This was often expressed as follows:

$$\text{For each } x \in R \text{ with } x > 0 \text{ and for each } y \in \mathbb{R},\ y = \ln x \text{ if and only if } x = e^y.$$

Notice that this means that x is the input and y is the output for the natural logarithm function if and only if y is the input and x is the output for the exponential function. In essence, the inverse function (in this case, the exponential function) reverses the action of the original function (in this case, the natural logarithm function). In terms of ordered pairs (input-output pairs), this means that if (x, y) is an ordered pair for a function, then (y, x) is an ordered pair for its inverse. This idea of reversing the roles of the first and second coordinates is the basis for our definition of the inverse of a function.

Definition: Inverse of a Function

Let $f : A \to B$ be a function. The inverse of f, denoted by f^{-1}, is the set of ordered pairs $\{(b, a) \in B \times A \mid f(a) = b\}$. That is,

$$f^{-1} = \{(b, a) \in B \times A \mid f(a) = b\}.$$

If we use the ordered pair representation for f, we could also write

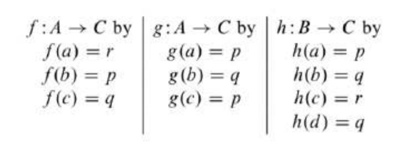
$$f^{-1} = \{(b, a) \in B \times A \mid (a, b) \in f\}.$$

Notice that this definition does not state that f^{-1} is a function. It is simply a subset of $B \times A$. After we study the material in Chapter 7, we will say that this means that f^{-1} is a **relation** from B to A. This fact, however, is not important to us now. We are mainly interested in the following question:

> **Under what conditions will the inverse of the function $f : A \to B$ be a function from B to A?**

Progress Check 6.24: Exploring the Inverse of a Function

Let $A = \{a, b, c\}$, $B = \{a, b, c, d\}$, and $C = \{p, q, r\}$. Define



$f : A \to C$ by	$g : A \to C$ by	$h : B \to C$ by
$f(a) = r$	$g(a) = p$	$h(a) = p$
$f(b) = p$	$g(b) = q$	$h(b) = q$
$f(c) = q$	$g(c) = p$	$h(c) = r$
		$h(d) = q$

1. Draw an arrow diagram for each function.
2. Determine the inverse of each function as a set of ordered pairs.
3. (a) Is f^{-1} a function from C to A? Explain.
   (b) Is g^{-1} a function from C to A? Explain.
   (c) Is h^{-1} a function from C to B? Explain.
4. Draw an arrow diagram for each inverse from Part (3) that is a function. Use your existing arrow diagram from Part (1) to draw this arrow diagram.
5. Make a conjecture about what conditions on a function $F : S \to T$ will ensure that its inverse is a function from T to S.

Answer

Add texts here. Do not delete this text first.

We will now consider a general argument suggested by the explorations in Progress Check 6.24. By definition, if $f : A \to B$ is a function, then f^{-1} is a subset of $B \times A$. However, f^{-1} may or may not be a function from B to A. For example, suppose that $s, t \in A$ with $s \neq t$ and $f(s) = f(t)$. This is represented in Figure 6.9.

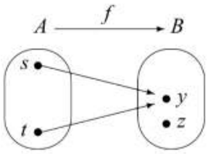


Figure 6.9: The Inverse Is Not a Function

In this case, if we try to reverse the arrows, we will not get a function from B to A. This is because $(y, s) \in f^{-1}$ and $(y, t) \in f^{-1}$ with $s \neq t$. Consequently, f^{-1} is not a function. This suggests that when f is not an injection, then f^{-1} is not a function.

Also, if f is not a surjection, then there exists a $z \in B$ such that $f(a) \neq z$ for all $a \in A$, as in the diagram in Figure 6.9. In other words, there is no ordered pair in f with z as the second coordinate. This means that there would be no ordered pair in f^{-1} with z as a first coordinate. Consequently, f^{-1} cannot be a function from B to A.

This motivates the statement in Theorem 6.25. In the proof of this theorem, we will frequently change back and forth from the input-output representation of a function and the ordered pair representation of a function. The idea is that if $G : S \to T$ is a function, then for $s \in S$ and $t \in T$,

$$G(s) = t \text{ if and only if } (s, t) \in G.$$

When we use the ordered pair representation of a function, we will also use the ordered pair representation of its inverse. In this case, we know that

$$(s, t) \in G \text{ if and only if } (t, s) \in G^{-1}.$$

Theorem 6.25.

Let A and B be nonempty sets and let $f : A \to B$. The inverse of f is a function from B to A if and only if f is a bijection.

Proof

Let A and B be nonempty sets and let $f : A \to B$. We will first assume that f is a bijection and prove that f^{-1} is a function from B to A. To do this, we will show that f^{-1} satisfies the two conditions of Theorem 6.22.

We first choose $b \in B$. Since the function f is a surjection, there exists an $a \in A$ such that $f(a) = b$. This implies that $(a, b) \in f$ and hence that $(b, a) \in f^{-1}$. Thus, each element of B is the first coordinate of an ordered pair in f^{-1}, and hence f^{-1} satisfies the first condition of Theorem 6.22.

To prove that f^{-1} satisfies the second condition of Theorem 6.22, we must show that each element of B is the first coordinate of exactly one ordered pair in f^{-1}. So let $b \in B$, $a_1, a_2 \in A$ and assume that

$$(b, a_1) \in f^{-1} \text{ and } (b, a_2) \in f^{-1}.$$

This means that \((a_1, b) \in f) and \((a_2, b) \in f). We can then conclude that

$$f(a_1) = b \text{ and } f(a_2) = b.$$

But this means that $f(a_1) = f(a_2)$. Since f is a bijection, it is an injection, and we can conclude that $a_1 = a_2$. This proves that b is the first element of only one ordered pair in f^{-1}. Consequently, we have proved that f^{-1} satisfies both conditions of Theorem 6.22 and hence that f^{-1} is a function from B to A.

We now assume that f^{-1} is a function B to A and prove that f is a bijection. First, to prove that f is an injection, we assume that $a_1, a_2 \in A$ and that $f(a_1) = f(a_2)$. We wish to show that $a_1 = a_2$. If we let $b = f(a_1) = f(a_2)$, we can conclude that

\((a_1, b) \in f) and \((a_2, b) \in f).

But this means that

$$(b, a_1) \in f^{-1} \text{ and } (b, a_2) \in f^{-1}.$$

Since we have assumed that f^{-1} is a function, we can conclude that $a_1 = a_2$. Hence, f is an injection.

Now to prove that f is a surjection, we choose $b \in B$ and will show that there exists an $a \in A$ such that $f(a) = b$. Since f^{-1} is a function, b must be the first coordinate of some ordered pair in f^{-1}. Consequently, there exists an $a \in A$ such that

$$(b, a) \in .f^{-1}.$$

Now this implies that $(a, b) \in f$ and hence that $f(a) = b$. This proves that f is a surjection. Since we have also proved that f is an injection, we conclude that f is a bijection.

Inverse Function Notation

In the situation where $f : A \to B$ is a bijection and f^{-1} is a function from B to A, we can write $f^{-1} : B \to A$. In this case, we frequently say that f is an **invertible function**, and we usually do not use the ordered pair representation for either f or f^{-1}. Instead of writing $(a, b) \in f$, we write $f(a) = b$, and instead of writing $(b, a) \in .f^{-1}$, we write $f^{-1}(b) = a$. Using the fact that $(a, b) \in f$ if and only if $(b, a) \in .f^{-1}$, we can now write $f(a) = b$ if and only if $f^{-1}(b) = a$. We summarize this in Theorem 6.26.

Theorem 6.26

Let A and B be nonempty sets and let $f : A \to B$ to be a bijection. Then $f^{-1} : B \to A$ is a function, and for every $a \in A$ and $b \in B$.

$$f(a) = b \text{ if and only if } f^{-1}(b) = a.$$

Example 6.27: Inverse Function Notation

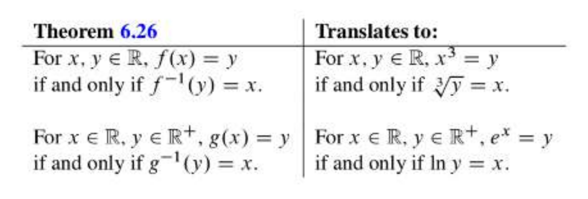
For an example of the use of the notation in Theorem 6.26, let $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$. Define

$$f : \mathbb{R} \to \mathbb{R} \text{ by } f(x) = x^3; \text{ and } g : \mathbb{R} \to \mathbb{R}^+ \text{ by } g(x) = e^x.$$

Notice that $\mathbb{R}^+$ is the codomain of g. We can then say that both f and g are bijections. Consequently, the inverses of these functions are also functions. In fact,

$$f^{-1} : \mathbb{R} \to \mathbb{R} \text{ by } f^{-1}(y) = \sqrt[3]{y}; \text{ and } g^{-1} : \mathbb{R}^+ \to \mathbb{R} \text{ by } g^{-1}(y) = \text{In} y.$$

For each function (and its inverse), we can write the result of Theorem 6.26 as follows:



Theorem 6.26	**Translates to:**
For $x, y \in \mathbb{R}$, $f(x) = y$ if and only if $f^{-1}(y) = x$.	For $x, y \in \mathbb{R}$, $x^3 = y$ if and only if $\sqrt[3]{y} = x$.
For $x \in \mathbb{R}$, $y \in \mathbb{R}^+$, $g(x) = y$ if and only if $g^{-1}(y) = x$.	For $x \in \mathbb{R}$, $y \in \mathbb{R}^+$, $e^x = y$ if and only if $\ln y = x$.

Theorems about Inverse Functions

The next two results in this section are two important theorems about inverse functions. The first is actually a corollary of Theorem 6.26.

Corollary 6.28.

Let A and B be nonempty sets and let $f : A \to B$ be a bijection. Then

1. For every x in A, $(f^{-1} \circ f)(x) = x$).
2. For every y in B, $(f \circ f^{-1})(y) = y$).

Proof

Let A and B be nonempty sets and assume that $f : A \to B$ is a bijection. So let $x \in A$ and let $f(x) = y$. By Theorem 6.26, we can conclude that $f^{-1}(y) = x$. Therefore,

Extra close brace or missing open brace

Hence, for each $x \in A$, $(f^{-1} \circ f)(x) = x$).

The proof that for each y in B, $(f \circ f^{-1})(y) = y$) is Exercise (4).

Example 6.27 (continued)

For the cubing function and the cube root function, we have seen that

For $x, y \in \mathbb{R}$, $x^3 = y$ if and only if $\sqrt[3]{y} = x$.

Notice that

- If we substitute $x^3 = y$ into the equation $\sqrt[3]{y} = x$, we obtain $\sqrt[3]{x^3} = x$.
- If we substitute $\sqrt[3]{y} = x$ into the equation $x^3 = y$, we obtain $(\sqrt[3]{y})^3 = y$.

This is an illustration of Corollary 6.28. We can see this by using $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$ and $f^{-1} : \mathbb{R} \to \mathbb{R}$ defined by $f^{-1}(y) = \sqrt[3]{y}$. Then $f^{-1} \circ f : \mathbb{R} \to \mathbb{R}$ and $f^{-1} \circ f = I_{\mathbb{R}}$,

Extra close brace or missing open brace

Similarly, the equation $(\sqrt[3]{y})^3 = y$ for each $y \in \mathbb{R}$ can be obtained from the fact that for each $y \in \mathbb{R}$, $(f \circ f^{-1})(y) = y$).

We will now consider the case where $f : A \to B$ and $g : B \to C$ are both bijections. In this case, $f^{-1} : B \to A$ and $g^{-1} : C \to B$. Figure 6.10 can be used to illustrate this situation.

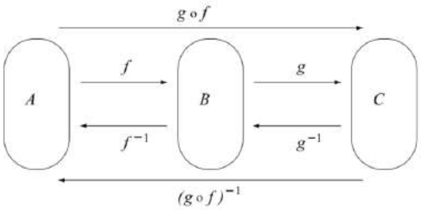


Figure 6.10: Composition of Two Bijections

By Theorem 6.20, $g \circ f : A \to C$ is also a bijection. Hence, by Theorem 6.25, $(g \circ f)^{-1}$ is a function and, in fact, $(g \circ f)^{-1} : C \to A$. Notice that we can also form the composition of g^{-1} followed by f^{-1} to get $f^{-1} \circ g^{-1} : C \to A$. Figure 6.10 helps illustrate the result of the next theorem.

Theorem 6.29.

Let $f : A \to B$ and $g : B \to C$ be bijections. Then $g \circ f$ is a bijection and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof

Let $f : A \to B$ and $g : B \to C$ be bijections. Then $f^{-1} : B \to A$ and $g^{-1} : C \to B$. Hence, $f^{-1} \circ g^{-1} : C \to A$. Also, by Theorem 6.20, $g \circ f : A \to C$ is a bijection, and hence $(g \circ f)^{-1} : C \to A$. We will now prove that for each $z \in C$, $(g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z)$.

Let $z \in C$. Since the function g is a surjection, there exists a $y \in B$ such that

$$g(y) = z. \tag{6.5.3}$$

Also, since f is a surjection, there exists an $x \in A$ such that

$$f(x) = y. \tag{6.5.4}$$

Now these two equations can be written in terms of the respective inverse functions as

Extra close brace or missing open brace

$$f^{-1}(y) = x. \tag{6.5.5}$$

Using equations (6.5.5) and (6.5.6), we see that

$$\begin{aligned} f^{-1} \circ g^{-1}(z) &= f^{-1}(g^{-1}(z)) \\ &= f^{-1}(y) \qquad (6.5.6) \\ &= x \end{aligned}$$

Using equations (6.5.3) and (6.5.4) again, we see that $(g \circ f)(x) = z$. However, in terms of the inverse function, this means that

$$(g \circ f)^{-1}(z) = x. \tag{6.5.7}$$

Comparing equations (6.5.7) and (6.5.8), we have shown that for all $z \in C$, $(g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z)$. This proves that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

? Exercise 6.5

1. Let $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$.
   (a) Construct an example of a function $f : A \to B$ that is not a bijection. Write the inverse of this function as a set of ordered pairs. Is the inverse of f a function? Explain. If so, draw an arrow diagram for f and f^{-1}.
   (b) Construct an example of a function $g : A \to B$ that is a bijection. Write the inverse of this function as a set of ordered pairs. Is the inverse of g a function? Explain. If so, draw an arrow diagram for g and g^{-1}.
2. Let $S = \{a, b, c, d\}$. Define $f : S \to S$ by defining f to be the following set of ordered pairs.

   $$f = \{(a, c), (b, b), (c, d), (d, a)\} \tag{6.5.8}$$

   (a) Draw an arrow diagram to represent the function f. Is the function fa bijection?
   (b) Write the inverse of f as a set of ordered pairs. Is f^{-1} a function? Explain.
   (c) Draw an arrow diagram for f^{-1} using the arrow diagram from Exercise (2a).
   (d) Compute $(f^{-1} \circ f)(x)$ and $(f \circ f^{-1}(x)$ for each x in S. What theorem does this illustrate?
3. Inverse functions can be used to help solve certain equations. The idea is to use an inverse function to undo the function.
   (a) Since the cube root function and the cubing function are inverses of each other, we can often use the cube root function to help solve an equation involving a cube. For example, the main step in solving the equation

   $$(2t - 1)^3 = 20 \tag{6.5.9}$$

   is to take the cube root of each side of the equation. This gives
   \[\begin{array} {rcl} {\sqrt[3]{(2t - 1)^3} &= & {\sqrt[3]{20}} \ {2t - 1} &= &{\sqrt[3]{20}.} \end{array}\]
   Explain how this step in solving the equation is a use of Corollary 6.28.

   (b) A main step in solving the equation \(e^{2t - 1} = 20} is to take the natural logarithm of both sides of this equation. Explain how this step is a use of Corollary 6.28, and then solve the resulting equation to obtain a solution for t in terms of the natural logarithm function.
   (c) How are the methods of solving the equations in Exercise (3a) and Exercise (3b) similar?
4. Prove Part (2) of Corollary 6.28. Let A and B be nonempty sets and let $f : A \to B$ be a bijection. Then for every y in B, $(f \circ f^{-1}(y) = y$.
5. In Progress Check 6.6 on page 298, we defined the identity function on a set. The **identity function on the set** T, denoted by I_T, is the function $I_T : T \to T$ defined by $I_T(t) = t$ for every t in T. Explain how Corollary 6.28 can be stated using the concept of equality of functions and the identity functions on the sets A and B.
6. Let $f : A \to B$ and $g : B \to A$. Let I_A and I_B be the identity functions on the sets A and B, respectively. Prove each of the following:
   (a) If $g \circ f = I_A$, then f is an injection.
   (b) If $g \circ g = I_B$, then f is a surjection.
   (c) If $g \circ f = I_A$ and $g \circ g = I_B$, then f and g are bijections and $g = f^{-1}$.
7. (a) Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = e^{-x^2}$. Is the inverse of f a function? Justify your conclusion.
   (b) Let $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \geq 0\}$. Define $g : \mathbb{R}^* \to (0, 1]$ by $g(x) = e^{-x^2}$. Is the inverse of g a function? Justify your conclusion.
8. (a) Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. Explain why the inverse of f is not a function.
   (b) Let $\mathbb{R}^* = \{t \in \mathbb{R} \mid t \geq 0\}$. Define $g : \mathbb{R}^* \to \mathbb{R}^*$ by $g(x) = x^2$. Explain why this squaring function (with a restricted domain and codomain) is a bijection.

(c) Explain how to define the square root function as the inverse of the function in Exercise (8b).
(d) True or false: $(\sqrt{x})^2 = x$ for all $x \in \mathbb{R}$ such that $x \geq 0$.
(e) True or false: $\sqrt{x^2} = x$ for all $x \in \mathbb{R}$.

9. Prove the following:
   If $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is also a bijection.
10. For each natural number k, let A_k be a set, and for each natural number n, let $f_n : A_n \to A_{n+1}$.
    For example, $f_1 = A_1 \to A_2$, $f_1 = A_1 \to A_2$, $f_2 = A_2 \to A_3$, $f_3 = A_3 \to A_4$, and so on.
    Use mathematical induction to prove that for each natural number n with $n \geq 2$, if f_1, f_2, ..., f_n are all bijections, then $f_n \circ f_{n-1} \circ \cdots \circ f_2 \circ f_1$ is a bijection and
    \[(f_n \circ f_{n - 1} \circ \cdot\cdot\cdot \circ f_2 \circ f_1)^{-1} = f_{1}^{-1} \cdot f_{2}^{-1} \cdot \cdot\cdot\cdot \circ f_{n - 1}^{-1} \circ f_{n}^{-1}
    Note: This is an extension of Theorem 6.29. In fact, Theorem 6.29 is the basis step of this proof for $n = 2$.
11. $a)Define$\($f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 - 4$ for all $x \in \mathbb{R}$. Explain why the inverse of the function f is not a function.
    (b) Let $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \geq 0\}$ and let $T = \{y \in \mathbb{R} \mid y \geq -4\}$. Define $F : \mathbb{R}^* \to T$ by $F(x) = x^2 - 4$ for all $x \in \mathbb{R}^*$. Explain why the inverse of the function F is a function and find a formula for $F^{-1}(y)$, where $y \in T$.
12. Let $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.
    (a) Define $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $f(x) = x^2 + 4$ (mod 5) for all $x \in \mathbb{Z}_5$. Write the inverse of f as a set of ordered pairs and explain why f^{-1} is not a function.
    (b) Define $g : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $g(x) = x^3 + 4$ (mod 5) for all $x \in \mathbb{Z}_5$. Write the inverse of g as a set of ordered pairs and explain why g^{-1} is not a function.
    (c) Is it possible to write a formula for $g^{-1}(y)$, where $y \in \mathbb{Z}_5$? The answer to this question depends on whether or not is possible to define a cube root of elements of $\mathbb{Z}_5$. Recall that for a real number x, we define the cube root of x to the real number y such that $y^3 = x$. That is,

    $$y = \sqrt[3]{x} \text{ if and only if } y^3 = x. \tag{6.5.10}$$

    Using this idea, is it possible to define the cube root of each number in $\mathbb{Z}_5$? If so, what is $\sqrt[3]{0}$, $\sqrt[3]{1}$, $\sqrt[3]{2}$, $\sqrt[3]{3}$, and $\sqrt[3]{4}$.
    (d) Now answer th equestion posed at the beginning of Part (c). If possible, determine a formula for $g^{-1}(y)$ where $g^{-1} : \mathbb{Z}_5 \to \mathbb{Z}_5$.

Explorations and Activities

13. **Constructing an Inverse Function.** If $f : A \to B$ is a bijection, then we know that its inverse is a function. If we are given a formula for the function f, it may be desirable to determine a formula for the function f^{-1}. This can sometimes be done, while at other times it is very difficult or even impossible.
    Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x^3 - 7$. A graph of this function would suggest that this function is a bijection.

    (a) Prove that the function f is an injection and a surjection.

    Let $y \in \mathbb{R}$. One way to prove that f is a surjection is to set $y = f(x)$ and solve for x. If this can be done, then we would know that there exists an $x \in \mathbb{R}$ such that $f(x) = y$. For the function f, we are using x for the input and y for the output. By solving for x in terms of y, we are attempting to write a formula where y is the input and x is the output. This formula represents the inverse function.

    (b) Solve the equation $y = 2x^3 - 7$ for x. Use this to write a formula for $f^{-1}(y)$, where $f^{-1} : \mathbb{R} \to \mathbb{R}$.
    (c) Use the result of Part (13b) to verify that for each $x \in \mathbb{R}$, $f^{-1}(f(x)) = x$ and for each $y \in \mathbb{R}$, $f(f^{-1}(y)) = y$.

    Now let $\mathbb{R}^+ = \{y \in \mathbb{R} \mid y > 0\}$. Define $g : \mathbb{R} \to \mathbb{R}^+$ by $g(x) = e^{2x-1}$.

    (d) Set $y = e^{2x-1}$ and solve for x in terms of y.
    (e) Use your work in Exercise (13d) to define a function $h : \mathbb{R}^+ \to \mathbb{R}$.
    (f) For each $x \in \mathbb{R}$, determine $(h \circ g)(x)$ and for each $y \in \mathbb{R}^+$, determine $(g \circ h)(y)$.
    (g) Use Exercise (6) to explain why $h = g^{-1}$.

14. **The Inverse Sine Function.** We have seen that in order to obtain an inverse function, it is sometimes necessary to restrict the domain (or the codomain) of a function.

(a) Let $f:\mathbb{R}\to\mathbb{R}$ be defined by $f(x)=sinx$. Explain why the inverse of the function f is not a function. (A graph may be helpful.)

Notice that if we use the ordered pair representation, then the sine function can be represented as

$$f=\{(x,y)\in\mathbb{R}\to\mathbb{R}\mid y=sinx\}. \tag{6.5.11}$$

If we denote the inverse of the sine function by $\sin^{-1}$, then

$$f^{-1}=\{(y,x)\in\mathbb{R}\to\mathbb{R}\mid y=sinx\}. \tag{6.5.12}$$

Part (14a) proves that f^{-1} is not a function. However, in previous mathematics courses, we frequently used the "inverse sine function." This is not really the inverse of the sine function as defined in Part (14a) but, rather, it is the inverse of the sine function **restricted to the domain** $[-\frac{\pi}{2},\frac{\pi}{2}]$.

(b) Explain why the function $F:[-\frac{\pi}{2},\frac{\pi}{2}]\to[-1,1]$ defined by $F(x)=sinx$ is a bijection.

The inverse of the function in Part (14b) is itself a function and is called the inverse sine function (or sometimes the arcsine function).

(c) What is the domain of the inverse sine function? What are the range and codomain of the inverse sine function?

Let us now use $F(x)=\sin(x)$ to represent the restricted sine function in Part (14b). Therefore, $F^{-1}(x)=\sin^{-1}(x)$ can be used to represent the inverse sine function. Observe that

$$F:[-\frac{\pi}{2},\frac{\pi}{2}]\to[-1,1] \text{ and } F^{-1}:[-1,1]\to[-\frac{\pi}{2},\frac{\pi}{2}]. \tag{6.5.13}$$

(d) Using this notation, explain why
$\sin^{-1}y=x$ if and only if [$y=\sin\,x$ and $-\frac{\pi}{2}\le x\le\frac{\pi}{2}$];
$\sin(\sin^{-1}(y))=y$ for all $y\in[-1,1]$; and
$\sin^{-1}(\sin(x))=x$ for all $x\in[-\frac{\pi}{2},\frac{\pi}{2}]$.

Answer

Add texts here. Do not delete this text first.

This page titled 6.5: Inverse Functions is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

6.6: Functions Acting on Sets

Preview Activity 1 (Functions and Sets)

Let $S = \{a, b, c, d\}$ and $T = \{s, t, u\}$. Define $f : S \to T$ by

$$f(a) = s\ f(b) = t\ f(c) = t\ f(d) = s$$

1. Let $A = \{a, c\}$ and $B = \{a, d\}$. Notice that A and B are subsets of S. Use the roster method to specify the elements of the following two subsets of T:

   (a) $\{f(x) \mid x \in A\}$
   (b) $\{f(x) \mid x \in B\}$
2. Let $C = \{s, t\}$ and $D = \{s, u\}$. Notice that C and D are subsets of T. Use the roster method to specify the elements of the following two subsets of S:

   (a) $\{x \in S \mid f(x) \in C\}$
   (b) $\{x \in S \mid f(x) \in D\}$

   Now let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^2$, for each $x \in \mathbb{R}$.
3. Let $A = \{1, 2, 3, -1\}$. Use the roster method to specify the elements of the set $\{g(x) \mid x \in A\}$.
4. Use the roster method to specify the elements of each of the following sets:

   (a) $\{x \in \mathbb{R} \mid g(x) = 1\}$
   (b) $\{x \in \mathbb{R} \mid g(x) = 9\}$
   (c) $\{x \in \mathbb{R} \mid g(x) = 15\}$
   (d) $\{x \in \mathbb{R} \mid g(x) = -1\}$
5. Let $B = \{1, 9, 15, -1\}$. Use the roster method to specify the elements of the set
   \{\x \in \mathbb{R}\ |\ g(x) \in B\}\).

Preview Activity 2 (Functions and Intervals)

Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^2$, for each $x \in \mathbb{R}$.

1. We will first determine where g maps the closed interval [1, 2]. (Recall that $[1, 2] = \{x \in R \mid 1 \le x \le 2\}$.) That is, we will describe, in simpler terms, the set $\{g(x) \mid x \in [1, 2]\}$. This is the set of all images of the real numbers in the closed interval [1, 2].

   (a) Draw a graph of the function g using $-3 \le x \le 3$.
   (b) On the graph, draw the vertical lines $x = 1$ and $x = 2$ from the x-axis to the graph. Label the points $P(1, f(1))$ and $Q(2, f(2))$ on the graph.
   (c) Now draw horizontal lines from the points P and Q to the y-axis. Use this information from the graph to describe the set $\{g(x) \mid x \in [1, 2]\}$ in simpler terms. Use interval notation or set builder notation.
2. We will now determine all real numbers that g maps into the closed interval [1, 4]. That is, we will describe the set $\{x \in \mathbb{R} \mid g(x) \in [1, 4]\}$ in simpler terms. This is the set of all preimages of the real numbers in the closed interval [1, 4].
   (a) Draw a graph of the function g using $-3 \le x \le 3$.
   (b) On the graph, draw the horizontal lines $y = 1$ and $y = 4$ from they-axis to the graph. Label all points where these two lines intersect the graph.
   (c) Now draw vertical lines from the points in Part (2) to the x-axis, and then use the resulting information to describe the set $\{x \in \mathbb{R} \mid g(x) \in [1, 4]\}$ in simpler terms. (You will need to describe this set as a union of two intervals. Use interval notation or set builder notation.)

Functions Acting on Sets

In our study of functions, we have focused on how a function "maps" individual elements of its domain to the codomain. We also studied the preimage of an individual element in its codomain. For example, if $f : \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = x^2$, for each $x \in \mathbb{R}$, then

- $f(2) = 4$. We say that f maps 2 to 4 or that 4 is the image of 2 under the function f.

- Since $f(2) = 4$ implies that $x = 2$ or $x = -2$, we say that the preimages of 4 are 2 and -2 or that the set of preimages of 4 is {-2, 2}.

For a function $f : S \to T$, the next step is to consider subsets of S or T and what corresponds to them in the other set. We did this in the Preview Activities. We will give some definitions and then revisit the examples in the Preview Activities in light of these definitions. We will first consider the situation where A is a subset of S and consider the set of outputs whose inputs are from A. This will be a subset of T.

Definition

Let $f : S \to T$. If $A \subseteq S$, then the **image of A under f** is the set $f(A)$, where

$$f(A) = \{f(x) \mid x \in A\}.$$

If there is no confusion as to which function is being used, we call $f(A)$ **the image of A.**

We now consider the situation in which C is a subset of T and consider the subset of A consisting of all elements of T whose outputs are in C.

Definition

Let $f : S \to T$. If $C \subseteq T$, then the **preimage of C under f** is the set $f^{-1}(C)$, where

$f^{-1}(C) = \{x \in S \mid f(x) \in C\}$.

If there is no confusion as to which function is being used, we call $f^{-1}(C)$ **the preimage of C**. The preimage of the set C under f is also called the **inverse image of C under f**.

Notice that the set $f^{-1}(C)$ is defined whether or not f^{-1} is a function.

Progress Check 6.30 (Preview Activity 6.6.1 Revisited)

Let $S = \{a, b, c, d\}$ and $T = \{s, t, u\}$. Define $f : S \to T$ by

$$f(a) = s \; f(b) = t \; f(c) = t \; f(d) = s.$$

Let $A = \{a, c\}$, $B = \{a, d\}$, $C = \{s, t\}$, and $D = \{s, u\}$.

Use your work in Preview Activity 6.6.1 to determine each of the following sets:

1. $f(A)$
2. $f(B)$
3. $f^{-1}(C)$
4. $f^{-1}(D)$

Answer

Add texts here. Do not delete this text first.

Example 6.31 (Images and Preimages of Sets)

Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^2$, for each $x \in \mathbb{R}$. The following results are based on the examples in Preview Activity 6.6.1 and Preview Activity 6.6.2.

- Let $A = \{1, 2, 3, -1\}$. Then $f(A) = \{1, 4, 9\}$.
- Let $B = \{1, 9, 15, -1\}$. Then $f^{-1}(B) = \{-\sqrt{15}, -3, -1, 1, 3, \sqrt{15}\}$.

The graphs from Preview Activity 6.6.2 illustrate the following results:

- If T is the closed interval [1, 2], then the image of the set T is

$$\begin{aligned} f(T) &= \{f(x) \mid x \in [1, 2]\} \\ &= [1, 4]. \end{aligned} \tag{6.6.1}$$

- If C is the closed interval [1, 4], then the preimage of the set C is

$$f^{-1}(C) = \{x \in \mathbb{R} \mid f(x) \in [1,4]\} = [-2,-1] \cup [1,2]. \tag{6.6.2}$$

Set Operations and Functions Acting on Sets

We will now consider the following situation: Let S and T be sets and let f be a function from S to T. Also, let A and B be subsets of S and let C and D be subsets of T. In the remainder of this section, we will consider the following situations and answer the questions posed in each case.

- The set $A \cap B$ is a subset of S and so $f(A \cap B$ is a subset of T. In addition, $f(A)$ and $f(B)$ are subsets of T. Hence, $f(A) \cap f(B)$ is a subset of T.

  Is there any relationship between $f(A \cap B$ and $f(A) \cap f(B)$?
- The set $A \cup B$ is a subset of S and so $f(A \cup B$ is a subset of T. In addition, $f(A)$ and $f(B)$ are subsets of T. Hence, $f(A) \cup f(B)$ is a subset of T.

  Is there any relationship between $f(A \cup B$ and $f(A) \cup f(B)$?
- The set $C \cap D$ is a subset of T and so $f^{-1}(C \cap D)$ is a subset of S. In addition, $f^{-1}(C)$ and $f^{-1}(D)$ are subsets of S. Hence, $f^{-1}(C)$ $\cap f^{-1}(D)$ is a subset of S.

  Is there any relationship between the sets $f^{-1}(C \cap D)$ and $f^{-1}(C) \cap f^{-1}(D)$?
- The set $C \cup D$ is a subset of T and so $f^{-1}(C \cup D)$ is a subset of S. In addition, $f^{-1}(C)$ and $f^{-1}(D)$ are subsets of S. Hence, $f^{-1}(C)$ $\cup f^{-1}(D)$ is a subset of S.

  Is there any relationship between the sets $f^{-1}(C \cup D)$ and $f^{-1}(C) \cup f^{-1}(D)$?

These and other questions will be explored in the next progress check.

? Progress check 6.32 (set operations and functions acting on sets)

In Section 6.2, we introduced functions involving congruences. For example, if we let

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}.$$

then we can define $f : \mathbb{Z}_8 \to \mathbb{Z}_8$ by $f(x) = r$, where $(x^2 + 2) \equiv r$ (mod 8) and $r \in \mathbb{Z}_8$. Moreover, we shortened this notation to

$$f(x) = (x^2 + 2) \text{ (mod 8)}$$

We will use the following subsets of $\mathbb{Z}_8$:

$$A = \{1, 2, 4\} \; B = \{3, 4, 6\} \; C = \{1, 2, 3\} \; D = \{3, 4, 5\}$$

1. Verify that $f(0) = 2$, $f(1) = 3$, $f(2) = 6$, and $f(3) = 3$. Then determine $f(4)$, $f(5)$, $f(6)$ and $f(7)$.
2. Determine $f(A)$, $F = f(A = B)$, $f^{-1}(C)$, and $f^{-1}(D)$.
3. For each of the following, determine the two subsets of $\mathbb{Z}_8$ and then determine if there is a relationship between the two sets. For example, $A \cap B = \{4\}$ and since $f(4) = 2$, we see that $f(A \cap B) = \{2\}$.

   (a) $f(A \cap B)$ and $f(A) \cap f(B)$
   (b) $f(A \cup B)$ and $f(A) \cup f(B)$
   (c) $f^{-1}(C \cap D)$ and $f^{-1}(C) \cap f^{-1}(D)$
   (d) $f^{-1}(C \cup D)$ and $f^{-1}(C) \cup f^{-1}(D)$
4. Notice that $f(A)$ is a subset of the codomain, $\mathbb{Z}_8$. Consequently, $f^{-1}(f(A))$ is a subset of the domain, $\mathbb{Z}_8$. Is there any relation between A and $f^{-1}f(A))$ in this case?
5. Notice that $f^{-1}(C)$ is a subset of the codomain, $\mathbb{Z}_8$. Consequently, $f(f^{-1}(f(C))$ is a subset of the domain, $\mathbb{Z}_8$. Is there any relation between C and $f(f^{-1}f(C))$ in this case?

Answer

Add texts here. Do not delete this text first.

✓ Example 6.33 (Set Operations and Functions Acting on Sets)

Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 + 2$ for all $x \in \mathbb{R}$. It will be helpful to use the graph shown in Figure 6.11.

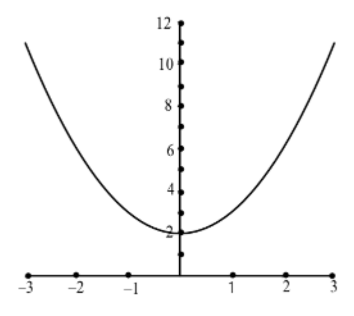


Figure 6.11: Graph for Example 6.33

We will use the following closed intervals:

$$A = [0, 3]\ B = [-2, 1]\ C = [2, 6]\ D = [0, 3].$$

1. Verify that $f(A) = [2, 11]$, $f(B) = [2, 6]$, $f^{-1}(C) = [-2, 2]$, and that $f^{-1}(D) = [-1, 1]$.
2. (a) Explain why $f(A \cap B) = [2, 3]$ and $f(A) \cap f(B) = [2, 6]$. So in this case, $f(A \cap B) \subsetneq f(A) \cap f(B)$.
   (b) Explain why $f(A \cup B) = [2, 11]$ and $f(A) \cup f(B) = [2, 11]$. So in this case, $f(A \cup B) \subseteq f(A) \cup f(B)$.
   (c) Explain why $f^{-1}(C \cap D) = [-1, 1]$ and $f^{-1}(C) \cap f^{-1}(D) = [-1, 1]$. So in this case, $f^{-1}(C \cap D) \subseteq f^{-1}(C) \cap f^{-1}(D)$.
   (d) Explain why $f^{-1}(C \cup D) = [-2, 2]$ and $f^{-1}(C) \cap f^{-1}(D) = [-2, 2]$. So in this case, $f^{-1}(C \cup D) \subseteq f^{-1}(C) \cup f^{-1}(D)$.
3. Reacll that $A = [0, 3]$. Notice $f(A) = [2, 11]$ is a subset of the codomain, $\mathbb{R}$. Explain why $f^{-1}(f(A)) = [-3, 3]$. Since $f^{-1}f(A))$ is a subset of the domain, $\mathbb{R}$, we see that in this case, $A \subsetneq f^{-1}(f(A))$.
4. Reacll that $C = [2, 6]$. Notice $f^{-1}(C) = [-2, 2]$ is a subset of the codomain, $\mathbb{R}$. Explain why $f(f^{-1}f(C)) = [2, 6]$. Since $f^{-1}f(C))$ is a subset of the domain, $\mathbb{R}$, we see that in this case, $f(f^{-1}(C)) = C$.

The examples in Progress Check 6.32 and Example 6.33 were meant to illustrate general results about how functions act on sets. In particular, we investigated how the action of a function on sets interacts with the set operations of intersection and union. We will now state the theorems that these examples were meant to illustrate. Some of the proofs will be left as exercises.

Theorem 6.34.

Let $f : S \to T$ be a function and let A and B be subsets of S. Then

1. $f(A \cap B$ \subseteq f(A) \cap f(B)\)
2. $f(A \cup B$ = f(A) \cup f(B)\)

Proof

We will prove Part (1). The proof of Part (2) is Exercise (5).

Assume that $f : S \to T$ is a function and let A and B be subsets of S. We will prove that $f(A \cap B$ \subseteq f(A) \cap f(B)\) by proving that for all $y \in T$, if $y \in f(A \cap B)$, then $y \in f(A) \cap f(B)$.

We assume that $y \in f(A \cap B)$. This means that there exists an $x \in A \cap B$ such that $f(x) = y$. Since $x \in A \cap B$, we conclude that $x \in A$ and $x \in B$.

- Since $x \in A$ and $f(x) = y$, we conclude that $y \in f(A)$.
- Since $x \in B$ and $f(x) = y$, we conclude that $y \in f(B)$.

Since $x \in f(A)$ and $y \in f(B)$, $y \in f(A) \cap f(B)$. This proves that if $y \in f(A \cap B)$, then $y \in f(A) \cap f(B)$. Hence $f(A \cap B$ \subseteq f(A) \cap f(B)\).

Theorem 6.35

Let $f : S \to T$ be a function and let C and D be subsets of T. Then

1. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$
2. $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$

Proof

We will prove Part (2). The proof of Part (1) is Exercise (6).

Assume $f : S \to T$ is a function and that C and D are subsets of T. We will prove that $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$ by proving that each set is a subset of the other.

We start by letting x be an element of $f^{-1}(C \cup D)$. This means that $f(x)$ is an element of $C \cup D$. Hence,

$$f(x) \in C \text{ or } f(x) \in D$$

In the case where $f(x) \in C$, we conclude that $x \in f^{-1}(C)$, and hence that $x \in f^{-1}(C) \cup f^{-1}(D)$. In the case where $f(x) \in D$, we see that $x \in f^{-1}(D)$, and hence that $x \in f^{-1}(C) \cup f^{-1}(D)$. So in both cases, $x \in f^{-1}(C) \cup f^{-1}(D)$, and we have proved that $f^{-1}(C \cup D) \subseteq f^{-1}(C) \cup f^{-1}(D)$

We now let $t \in f^{-1}(C) \cup f^{-1}(D)$. This means that

$$t \in f^{-1}(C) \text{ or } t \in f^{-1}(D)$$

- In the case where $t \in f^{-1}(C)$, we conclude that $f(t) \in C$ and hence that $f(t) \in C \cup D$. This means that $t \in f^{-1}(C \cup D)$.
- Similarly, when $t \in f^{-1}(D)$, it follows that $f(t) \in D$ and hence that $f(t) \in C \cup D$. This means that $t \in f^{-1}(C \cup D)$.

These two cases prove that if $t \in f^{-1}(C) \cup f^{-1}(D)$, then $t \in f^{-1}(C \cup D)$. Therefore, $f^{-1}(C) \cup f^{-1}(D) \subseteq f^{-1}(C \cup D)$.

Since we have now proved that each of the two sets is a subset of the other set, we can conclude that $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.

Theorem 6.36.

Let $f : S \to T$ be a function and let A be a subset of S and let C be a subset of T. Then

1. $A \subseteq f^{-1}(f(A))$
2. $f(f^{-1}(C)) \subseteq C$

Proof

We will prove Part (1). The proof of Part (2) is Exercise (7).

To prove Part (1), we will prove that for all $a \in S$, if $a \in A$, then $a \in f^{-1}(f(A))$. So let $a \in A$. Then, by definition, $f(a) \in f(A)$. We know that $f(A) \subseteq T$, and so $f^{-1}(f(A)) \subseteq S$. Notice that

$$f^{-1}(f(A)) = \{x \in S \mid f(x) \in f(A)\}.$$

Since $f(a) \in f(A)$, we use this to conclude that $a \in f^{-1}(f(A)).Thisprovesthatif$\($a \in A$, then $a \in f^{-1}(f(A))$, and hence that $A \in f^{-1}(f(A))$

Exercise 6.6

1. Let $f : S \to T$. let A and B be subsets of S, and let C and D be subsets of T. For $x \in S$ and $y \in T$, carefully explain what it means to say that

   (a) $y \in f(A \cap B)$
   (b) $y \in f(A \cup B)$
   (c) $y \in f(A) \cap f(B)$
   (d) $y \in f(A) \cup f(B)$
   (e) $x \in f^{-1}(C \cap D)$

(f) $x \in f^{-1}(C \cup D)$
(g) $x \in f^{-1}(C) \cap f^{-1}(D)$
(h) $x \in f^{-1}(C) \cup f^{-1}(D)$

2. Let $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = -2x + 1$. Let

   $A = [2, 5]$ $B = [-1, 3]$ $C = [-2, 3]$ $D = [1, 4]$.

   Find each of the following:

   (a) $f(A)$
   (b) $f^{-1}(f(A))$
   (c) $f^{-1}(C)$
   (d) $f(f^{-1}(C))$
   (e) $f(A \cap B)$
   (f) $f(A) \cap f(B)$
   (g) $f^{-1}(C \cap D)$
   (h) $f^{-1}(C) \cap f^{-1}(D)$
3. Let $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $g(m, n) = 2^m 3^n$, let $A = \{1, 2, 3\}$, and let $C = \{1, 4, 6, 9, 12, 16, 18\}$. Find

   (a) $g(A \times A)$
   (b) $g^{-1}(C)$
   (c) $g^{-1}(g(A \times A))$
   (d) $g(g^{-1}(C))$
4. (a) Let $S = \{1, 2, 3, 4\}$. Define $F : S \to \mathbb{N}$ by $F(x) = x^2$ for each $x \in s$. What is the range of the function F and what is $F(S)$? How do these two sets compare?

   Now let A and B be sets and let $f : A \to B$ be an arbitrary function from A to B.

   (b) Explain why $f(A) = \text{range}(f)$.
   (c) Define a function $g : A \to f(A)$ by $g(x) = f(x)$ for all x in A. Prove that the function g is a surjection.
5. Prove Part (2) of Theorem 6.34.
   Let $f : S \to T$ be a function and let A and B be subsets of S. Then $f(A \cup B) = f(A) \cup f(B)$.
6. Prove Part (1) of Theorem 6.35.
   Let $f : S \to T$ be a function and let C and D be subsets of T. Then $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.
7. Prove Part (2) of Theorem 6.36.
   Let $f : S \to T$ be a function and let $C \subseteq T$. Then $f(f^{-1}(C)) \subseteq C$.
8. Let $f : S \to T$ and let A and B be subsets of S. Prove or disprove each of the following:

   (a) If $A \subseteq B$, then $f(A) \subseteq f(B)$.
   (b) If $f(A) \subseteq f(B)$, then $A \subseteq B$.
9. Let $f : S \to T$ and let C and D be subsets of T. Prove or disprove each of the following:

   (a) If $C \subseteq D$, then $f^{-1}(C) \subseteq f^{-1}(D)$.
   (b) If $f^{-1}(C) \subseteq f^{-1}(D)$, then $C \subseteq D$.
10. Prove or disprove:
    If $f : S \to T$ is a function and A and B are subsets of S, then
    $f(A) \cap f(B) \subseteq f(A \cap B)$.
    Note: Part (1) of Theorem 6.34 states that $f(A \cap B) \subseteq f(A) \cap f(B)$.
11. If $f : S \to T$ is a function, let $A \subseteq S$, and let $C \subseteq T$.
    (a) Part (1) of Theorem 6.36 states that $A \subseteq f^{-1}(f(A))$. Give an example where $f^{-1}(f(A))$\notsubseteq$A$.
    (b) Part (2) of Theorem 6.36 states that $f(f^{-1}(C)) \subseteq C$. Give an example where C\notsubseteq$f(f^{-1}(C))$.

12. Is the following proposition true or false? Justify your conclusion with a proof or a counterexample.
    If $f : S \to T$ is an injection and $A \subseteq S$, then $f^{-1}(f(A)) = A$.
13. Is the following proposition true or false? Justify your conclusion with a proof or a counterexample.
    If $f : S \to T$ is an injection and $C \subseteq T$, then $f^{-1}(f(C)) = C$.
14. Let (f: S \to T\). Prove that $f(A \cap B) = f(A) \cap f(B)$ for all subsets A and B of S if and only if f is an injection.

Answer

Add texts here. Do not delete this text first.

This page titled 6.6: Functions Acting on Sets is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

6.S: Functions (Summary)

Important Definitions

- Function, page 284
- Domain of a function, page 285
- Codomain of a function,page285
- Image of x under f, page 285
- preimage of y under f, page 285
- Independent variable, page 285
- Dependent variable, page 285
- Range of a function, page 287
- Image of a function, page 287
- Equal functions, page 298
- Sequence, page 301
- Injection, page 310
- One-to-one function, page 310
- Surjection, page 311
- Onto function, page 311
- Bijection, page 312
- One-to-one and onto, page 312
- Composition of f and g, page 325
- Composite function, page 325
- f followed by g, page 325
- Inverse of a function, page 338
- Image of a set under a function, page 351
- preimage of a set under a function, page 351

Important Theorems and Results about Functions

- Theorem 6.20. Let A, B and C be nonempty sets and let $f : A \to B$ and $g : B \to C$.

  1. If f and g are both injections, then $g \circ f$ is an injection.
  2. If f and g are both surjections, then $g \circ f$ is a surjection.
  3. If f and g are both bijections, then $g \circ f$ is a bijection.
- Theorem 6.21. Let A, B and C be nonempty sets and let $f : A \to B$ and $g : B \to C$.

  1. If $g \circ f : A \to C$ is an injection, then $f : A \to B$ is an injeciton.
  2. If $g \circ f : A \to C$ is a surjection, then $g : B \to C$ is a surjeciton.
- Theorem 6.22. Let A and B be nonempty sets and let f be a subset of $A \times B$ that satisfies the following two properties:

  - For every $a \in A$, there exists $b \in B$ such that $(a, b) \in f$; and
  - For every $a \in A$ and every $b, c \in B$, if $(a, b) \in f$ and $(a, c) \in f$, then $b = c$.

  If we use $f(a) = b$ whenever $(a, b) \in f$, then f is a function from A to B.
- Theorem 6.25. Let A and B be nonempty sets and let $f : A \to B$. The inverse of f is a function from B to A if and only if f is a bijection.
- Theorem 6.26. Let A and B be nonempty sets and let $f : A \to B$ be a bijection. Then $f^{-1} : B \to A$ is a function, and for every $a \in A$ and $b \in B$,
  $f(a) = b$ if and only if $f^{-1}(b) = a$.
- Corollary 6.28. Let A and B be nonempty sets and let $f : A \to B$ be a bijection. Then

  1. For every x in A, $(f^{-1} \circ f)(x) = x$.
  2. For every y in B, $(f \circ f^{-1}(y) = y$.

- Theorem 6.29. Let $f : A \to B$ and $g : B \to C$ be bijections. Then $g \circ f$ is a bijection and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
- Theorem 6.34. Let $f : S \to T$ be a function and let A and B be subsets of S. Then

    1. $f(A \cap B) \subseteq f(A) \cap f(B)$
    2. $f(A \cup B) = f(A) \cup f(B)$
- Theorem 6.35. Let $f : S \to T$ be a function and let C and D be subsets of T. Then

    1. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$
    2. $f^{-1}(C \cup D) = f^{-1}(C) \cap f^{-1}(D)$
- Theorem 6.36. Let $f : S \to T$ be a function and let $A\backslash(beasubsetof\backslash(S$ and let C be a subset of T. Then

    1. $A \subseteq f^{-1}(f(A))$
    2. $f(f^{-1}(C) \subseteq C$

This page titled 6.S: Functions (Summary) is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

CHAPTER OVERVIEW

7: Equivalence Relations

In Section 6.1, we introduced the formal definition of a function from one set to another set. The notion of a function can be thought of as one way of relating the elements of one set with those of another set (or the same set). A function is a special type of *relation* in the sense that each element of the first set, the domain, is “related” to exactly one element of the second set, the codomain. This idea of relating the elements of one set to those of another set using ordered pairs is not restricted to functions. For example, we may say that one integer, a , is related to another integer, b , provided that a is congruent to b modulo 3. Notice that this relation of congruence modulo 3 provides a way of relating one integer to another integer. However, in this case, an integer a is related to more than one other integer.

- 7.1: Relations
- 7.2: Equivalence Relations
- 7.3: Equivalence Classes
- 7.4: Modular Arithmetic
- 7.S: Equivalence Relations (Summary)

This page titled 7: Equivalence Relations is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

7.1: Relations

? PREVIEW ACTIVITY 7.1.1: The United States of America

Recall from Section 5.4 that the **Cartesian product** of two sets A and B, written $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. That is, $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$.

Let A be the set of all states in the United States and let

$$R = \{(x, y) \in A \times A \mid x \text{ and } y \text{ have a land border in common}\}.$$

For example, since California and Oregon have a land border, we can say that (California, Oregon) $\in R$ and (Oregon, California) $\in R$. Also, since California and Michigan do not share a land border, (California, Michigan) $\notin R$ and (Michigan, California) $\notin R$.

1. Use the roster method to specify the elements in each of the following sets:

   (a) $B = \{y \in A \mid (\text{Michigan}, y) \in R\}$
   (b) $C = \{x \in A \mid (x, \text{Michigan}) \in R\}$
   (c) $D = \{y \in A \mid (\text{Wisconsin}, y) \in R\}$
2. Find two different examples of two ordered pairs (x, y) and (y, z) such that $(x, y) \in R$, $(y, z) \in R$, but $(x, z) \notin R$, or explain why no such example exists. Based on this, is the following conditional statement true or false?

   For all $x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.
3. Is the following conditional statement true or false? Explain.

   For all $x, y \in A$, if $(x, y) \in R$ then $(y, x) \in R$.

? PREVIEW ACTIVITY 7.1.2: The Solution Set of an Equation with Two Variables

In Section 2.3, we introduced the concept of the **truth set of an open sentence with one variable.** This was defined to be the set of all elements in the universal set that can be substituted for the variable to make the open sentence a true proposition. Assume that x and y represent real numbers. Then the equation

$$4x^2 + y^2 = 16$$

is an open sentence with two variables. An element of the truth set of this open sentence (also called a solution of the equation) is an ordered pair (a, b) of real numbers so that when a is substituted for x and b is substituted for y, the predicate becomes a true statement (a true equation in this case). We can use set builder notation to describe the truth set S of this equation with two variables as follows:

$$S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid 4x^2 + y^2 = 16\}.$$

When a set is a truth set of an open sentence that is an equation, we also call the set the **solution set** of the equation.

1. List four different elements of the set S.
2. The graph of the equation $4x^2 + y^2 = 16$ in the xy-coordinate plane is an ellipse. Draw the graph and explain why this graph is a representation of the truth set (solutions set) of the equation $4x^2 + y^2 = 16$.
3. Describe each of the following sets as an interval of real numbers:

   (a) $A = \{x \in \mathbb{R} \mid \text{there exists a } y \in \mathbb{R} \text{ such that } 4x^2 + y^2 = 16\}$.
   (b) $B = \{y \in \mathbb{R} \mid \text{there exists an } x \in \mathbb{R} \text{ such that } 4x^2 + y^2 = 16\}$.

Introduction to Relations

In Section 6.1, we introduced the formal definition of a function from one set to another set. The notion of a function can be thought of as one way of relating the elements of one set with those of another set (or the same set). A function is a special type of

relation in the sense that each element of the first set, the domain, is “related” to exactly one element of the second set, the codomain.

This idea of relating the elements of one set to those of another set using ordered pairs is not restricted to functions. For example, we may say that one integer, a, is related to another integer, b, provided that a is congruent to b modulo 3. Notice that this relation of congruence modulo 3 provides a way of relating one integer to another integer. However, in this case, an integer a is related to more than one other integer. For example, since

$$5 \equiv 5 \text{ (mod 3)},\ 5 \equiv 2 \text{ (mod 3)}, \text{ and } 5 \equiv -1 \text{ (mod 3)},$$

we can say that 5 is related to 3, 5 is related to 2, and 5 is related to -1. Notice that, as with functions, each relation of the form $a \equiv b$ (mod 3) involves two integersa and b and hence involves an ordered pair (a, b), which is an element of $\mathbb{Z} \times \mathbb{Z}$.

Definition: relations

Let A and B be sets. A **relation** R **from the set** A **to the set** B is a subset of $A \times B$. That is, R is a collection of ordered pairs where the first coordinate of each ordered pair is an element of A, and the second coordinate of each ordered pair is an element of B.

A relation from the set A to the set A is called a **relation on the set** A. So a relation on the set A is a subset of $A \times A$.

In Section 6.1, we defined the domain and range of a function. We make similar definitions for a relation.

Definition: Domain and Range

If R is a relation from the set A to the set B, then the subset of A consisting of all the first coordinates of the ordered pairs in R is called the *domain* of R. The subset of B consisting of all the second coordinates of the ordered pairs in R is called the *range* of R.

We use the notation dom(R) for the domain of R and range(R) for the range of R. So using set builder notation,

$$\text{dom}(R) = \{u \in A \mid (u, y) \in R \text{ for at least one } y \in B\}$$

$$\text{range}(R) = \{v \in B \mid (x, v) \in R \text{ for at least one } x \in A\}.$$

Example 7.1: Domain and Range

A relation was studied in each of the Preview Activities for this section. For Preview Activity 2, the set $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid 4x^2 + y^2 = 16\}$ is a subset of $\mathbb{R} \times \mathbb{R}$ and, hence, S is a relation on $\mathbb{R}$. In Problem (3) of Preview Activity $7.1.2$, we actually determined the domain and range of this relation.

$$\text{dom}(S) = A = \{x \in \mathbb{R} \mid \text{there exists a } y \in \mathbb{R} \text{ such that } 4x^2 + y^2 = 16\}$$

$$\text{range}(S) = B = \{y \in \mathbb{R} \mid \text{there exists an } x \in \mathbb{R} \text{ such that } 4x^2 + y^2 = 16\}$$

So from the results in Preview Activity $7.1.2$, we can say that the domain of the relation S is the closed interval [-2, 2] and the range of S is the closed interval [-4, 4].

Progress Check 7.2: Examples of Relations

1. Let $T = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 64\}$.

   (a) Explain why T is a relation on $\mathbb{R}$.
   (b) Find all values of x such that $(x, 4) \in T$. Find all values of x such that $(x, 9) \in T$.
   (c) What is the domain of the relation T? What is the range of T?
   (d) Since T is a relation on $\mathbb{R}$, its elements can be graphed in the coordinate plane. Describe the graph of the relation T.
2. From Preview Activity $7.1.1$, A is the set of all states in the United States, and

$$R = \{(x, y) \in A \times A \mid x \text{ and } y \text{ have a border in common}\}. \tag{7.1.1}$$

(a) Explain why R is a relation on A.
(b) What is the domain of the relation R? What is the range of the relation R?
(c) Are the following statements true or false? Justify your conclusions.
i. For all $x, y \in A$, if $(x, y) \in R$, then $(y, x) \in R$.
ii. For all $x, y, z \in A$, if $(x, y) \in R$ and $(y, x) \in R$, then $(x, z) \in R$.

Answer

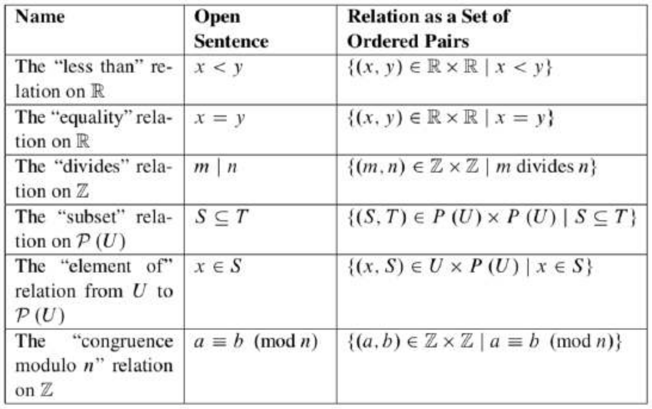
Add texts here. Do not delete this text first.

Some Standard Mathematical Relations

There are many different relations in mathematics. For example, two real numbers can be considered to be related if one number is less than the other number. We call this the "less than" relation on $\mathbb{R}$. If $x, y \in \mathbb{R}$ and x is less than y, we often write $x < y$. As a set of ordered pairs, this relation is $R_<$, where

\{R_{<} = \{(x, y) \in \mathbb{R} \times \mathbb{R}\ |\ x < y\}\).

With many mathematical relations, we do not write the relation as a set of ordered pairs even though, technically, it is a set of ordered pairs. Table 7.1 describes some standard mathematical relations.



Name	Open Sentence	Relation as a Set of Ordered Pairs
The "less than" relation on $\mathbb{R}$	$x < y$	$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$
The "equality" relation on $\mathbb{R}$	$x = y$	$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y\}$
The "divides" relation on $\mathbb{Z}$	$m \mid n$	$\{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divides } n\}$
The "subset" relation on $\mathcal{P}(U)$	$S \subseteq T$	$\{(S, T) \in P(U) \times P(U) \mid S \subseteq T\}$
The "element of" relation from U to $\mathcal{P}(U)$	$x \in S$	$\{(x, S) \in U \times P(U) \mid x \in S\}$
The "congruence modulo n" relation on $\mathbb{Z}$	$a \equiv b \pmod n$	$\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \pmod n\}$

Table 7.1: Standard Mathematical Relations

Notation for Relations

The mathematical relations in Table 7.1 all used a relation symbol between the two elements that form the ordered pair in $A \times B$. For this reason, we often do the same thing for a general relation from the set A to the set B. So if R is a relation from A to B, and $x \in A$ and $y \in B$, we use the notation

$$\begin{array}{lll} x\,R\,y & \text{to mean} & (x, y) \in R; \text{ and} \\ x \not R\, y & \text{to mean} & (x, y) \notin R. \end{array}$$

In some cases, we will even use a generic relation symbol for defining a new relation or speaking about relations in a general context. Perhaps the most commonly use symbol is "~", read "tilde" or "squiggle" or "is related to." When we do this, we will write

$$\begin{array}{lll} x \quad y & \text{means the same thing as} & (x, y) \in R; \text{ and} \\ x \nsim y & \text{means the same thing as} & (x, y) \notin R. \end{array} \tag{7.1.2}$$

? Progress Check 7.3: The Divides Relation

Whenever we have spoken about one integer dividing another integer, we have worked with the "divides" relation on $\mathbb{Z}$. In particular, we can write

$$D = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divides } n\}.$$

In this case, we have a specific notation for "divides," and we write

$$m \mid n \text{ if and only if } (m,n) \in D.$$

1. What is the domain of the "divides" relation? What is the range of the "divides" relation?
2. Are the following statements true or false? Explain.

   (a) For every nonzero integer a, $a \mid a$.
   (b) For all nonzero integers a and b, if $a \mid b$, then $b \mid a$.
   (c) For all nonzero integers a, b, and c,if $a \mid b$ and $b \mid c$, then $a \mid c$.

Answer

Add texts here. Do not delete this text first.

Functions as Relations

If we have a function $f : A \to B$, we can generate a set of ordered pairs f that is a subset of $A \times B$ as follows:

$$f = \{(a, f(a)) \mid a \in A\} \text{ or } f = \{(a,b) \in A \times B \mid b = f(a)\}.$$

This means that f is a relation from A to B. Since, dom$(f) = A$, we know that

(1) For every $a \in A$, there exists $a, b \in B$ such that $(a,b) \in f$.

When $(a,b) \in f$., we write $b = f(a)$. In addition, to be a function, each input can produce only one output. In terms of ordered pairs, this means that there will never be two ordered pairs (a,b) and $a,c)$ in the function f, where $a \in A$, $b, c \in B$, and $b \ = c$. We can formulate this as a conditional statement as follows:

(2) For every $a \in A$ and every $b, c \in B$, if $(a,b) \in f$ and $(a,c) \in f$, then $b = c$.

This means that a function f from A to B is a relation from A to B that satisfies conditions (1) and (2). (See Theorem 6.22 in Section 6.5.) Not every relation, however, will be a function. For example, consider the relation T in Progress Check 7.2.

? Progress Check 7.4: A Set of Ordered Pairs

Let $F = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$. The set F can then be considered to be relation on $\mathbb{R}$ since it is a subset of $\mathbb{R} \times \mathbb{R}$.

1. List five different ordered pairs that are in the set F.
2. Use the roster method to specify the elements of each of the following the sets:

   (a) $A = \{x \in \mathbb{R} \mid (x,4) \in F\}$
   (b) $B = \{x \in \mathbb{R} \mid (x,10) \in F\}$
   (c) $C = \{y \in \mathbb{R} \mid (5,y) \in F\}$
   (d) $D = \{y \in \mathbb{R} \mid (-3,y) \in F\}$
3. Since each real number x produces only one value of y for which $y = x^2$, the set F can be used to define a function from the set $\mathbb{R}$ to $\mathbb{R}$. Draw a graph of this function.

Answer

Add texts here. Do not delete this text first.

Visual Representations of Relations

In Progress Check 7.4, we were able to draw a graph of a relation as a way to visualize the relation. In this case, the relation was a function from $\mathbb{R}$ to $\mathbb{R}$. In addition, in Progress Check 7.2, we were also able to use a graph to represent a relation. In this case, the graph of the relation $T = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 64\}$ is a circle of radius 8 whose center is at the origin.

When R is a relation from a subset of the real numbers $\mathbb{R}$ to a subset of $\mathbb{R}$, we can often use a graph to provide a visual representation of the relation. This is especially true if the relation is defined by an equation or even an inequality. For example, if

$$R = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y \geq x^2\},$$

then we can use the following graph as a way to visualize the points in the plane that are also in this relation.

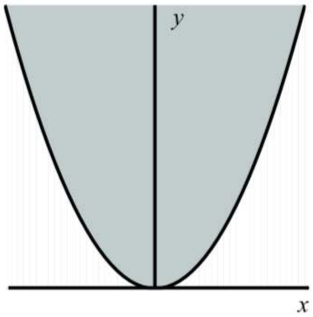


Figure 7.1: Graph of $y \geq x^2$

The points (x, y) in the relation R are the points on the graph of $y = x^2$ or are in the shaded region. This because for these points, $y \geq x^2$. One of the shortcomings of this type of graph is that the graph of the equation and the shaded region are actually unbounded and so we can never show the entire graph of this relation. However, it does allow us to see that the points in this relation are either on the parabola defined by the equation $y = x^2$ or are “inside” the parabola.

When the domain or range of a relation is infinite, we cannot provide a visualization of the entire relation. However, if A is a (small) finite set, a relation R on A can be specified by simply listing all the ordered pairs in R. For example, if $A = \{1, 2, 3, 4\}$, then

$$R = \{(1,1), (4,4), (1,3), (3,2), (1,2), (2,1)\}$$

is a relation on A. A convenient way to represent such a relation is to draw a point in the plane for each of the elements of A and then for each $(x, y) \in R$ (or $x\ R\ y$), we draw an arrow starting at the point x and pointing to the point y. If $(x, x) \in R$ (or $x\ R\ x$), we draw a loop at the point x. The resulting diagram is called a **directed graph** or a **digraph**. The diagram in Figure 7.2 is a digraph for the relation R.

In a directed graph, the points are called the **vertices**. So each element of A corresponds to a **vertex**. The arrows, including the loops, are called the **directed edges** of the directed graph. We will make use of these directed graphs in the next section when we study equivalence relations.

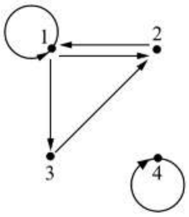


Figure 7.2: Directed Graph for a Relation

? Progress Check 7.5: The Directed Graph of a Relation

Let $A = \{1, 2, 3, 4, 5, 6\}$. Draw a directed graph for the following two relations on the set A. For each relation, it may be helpful to arrange the vertices of A as shown in Figure 7.3.

$R = \{(x, y) \in A \times A \mid x \text{ divides } y\}$, $T = \{(x, y) \in A \times A \mid x + y \text{ is even}\}$.

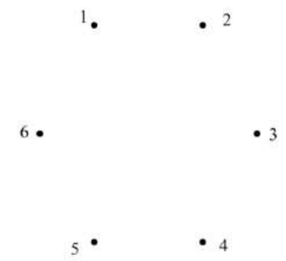


Figure 7.3: Vertices for A

Answer

Add texts here. Do not delete this text first.

Exercise 7.1

1. Let $A=\{a,b,c\}$, $B=\{p,q,r\}$, and let R be the set of ordered pairs defined by $R=\{(a,p),(b,q),(c,p),(a,q)\}$.

   (a) Use the roster method to list all the elements of $A\times B$. Explain why $A\times B$ can be considered to be a relation from A to B.
   (b) Explain why R is a relation from A to B.
   (c) What is the domain of R? What is the range of R?
2. Let $A=\{a,b,c\}$ and let $R=\{(a,a),(a,c),(b,b),(b,c),(c,a),(c,b)\}$ (so R is a relation on A). Are the following statements true or false? Explain.

   (a) For each $x\in A$, $x\ R\ x$.
   (b) For every $x,y\in A$, if $x\ R\ y$, then $y\ R\ x$.
   (c) For every $x,y,z\in A$, if $x\ R\ y$ and $y\ R\ z$, then $x\ R\ z$.
   (d) R is a function from A to A.
3. Let A be the set of all females citizens of the United States. Let D be the relation on A defined by

   $$D=\{(x,y)\in A\times A\mid x\text{ is a daughter of }y\}. \tag{7.1.3}$$

   That is, $x\ D\ y$ means that x is a daughter of y.

   (a) Describe those elements of A that are in the domain of D.
   (b) Describe those elements of A that are in the range of D.
   (c) Is the relation D a function from A to A? Explain.
4. Let U be a nonempty set, and let R be the “subset relation” on $\mathcal{P}(U)$. That is,

   $$R=\{(S,T)\in\mathcal{P}(U)\times\mathcal{P}(U)\mid S\subseteq T\}. \tag{7.1.4}$$

   (a) Write the open sentence $(S,T)\in R$ using standard subset notation.
   (b) What is the domain of this subset relation, R?
   (c) What is the range of this subset relation, R?
   (d) Is R a function from $\mathcal{P}(U)$ to $\mathcal{P}(U)$? Explain.
5. Let U be a nonempty set, and let R be the "element of" relation from U to $\mathcal{P}(U)$. That is,

   $$R=\{(x,S)\in U\times\mathcal{P}(U)\mid x\in S\}. \tag{7.1.5}$$

   (a) What is the domain of this “element of” relation, R?
   (b) What is the range of this "element of" relation, R?
   (c) Is R a function from U to $\mathcal{P}(U)$? Explain.

6. Let $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 100\}$.

   (a) Determine the set of all values of x such that $(x, 6) \in S$, and determine the set of all values of x such that $(x, 9) \in S$.
   (b) Determine the domain and range of the relation S and write each set using set builder notation.
   (c) Is the relation S a function from $\mathbb{R}$ to $\mathbb{R}$? Explain.
   (d) Since S is a relation on $\mathbb{R}$, its elements can be graphed in the coordinate plane. Describe the graph of the relation S. Is the graph consistent with your answers in Exercises (6a) through (6c)? Explain.
7. Repeat Exercise(6) using the relation on $\mathbb{R}$ defined by

$$S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = \sqrt{100 - x^2}\}. \tag{7.1.6}$$

   What is the connection between this relation and the relation in Exercise (6)?
8. Determine the domain and range of each of the following relations on $\mathbb{R}$ and sketch the graph of each relation.

   (a) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 10\}$
   (b) $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y^2 = x + 10\}$
   (c) $T = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid |x| + |y| = 10\}$
   (d) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 = y^2\}$
9. Let R be the relation on $\mathbb{Z}$ where for all $a, b \in \mathbb{Z}$, $a \; R \; b$ if and only if $|a - b| \le 2$.

   (a) Use set builder notation to describe the relation R as a set of ordered pairs.
   (b) Determine the domain and range of the relation R.
   (c) Use the roster method to specify these to fall integers x such that $x \; R \; 5$ and the set of all integers x such that $5 \; R \; x$.
   (d) If possible, find integers x and y such that $x \; R \; 8$, $8 \; R \; y$, but $x \not\!R \; y$.
   (e) If $a \in \mathbb{Z}$, use the roster method to specify the set of all $x \in \mathbb{Z}$ such that $x \; R \; a$.
10. Let $R_< = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$. This means that $R_<$ is the "less than" relation on $\mathbb{R}$.

   (a) What is the domain of the relation $R_<$?
   (b) What is the range of the relation $R_<$?
   (c) Is the relation $R_<$ a function from $\mathbb{R}$ to $\mathbb{R}$? Explain.

   Note: Remember that a relation is a set. Consequently, we can talk about one relation being a subset of another relation. Another thing to remember is that the elements of a relation are ordered pairs.

   Explorations and Activities
11. **The Inverse of a Relation**. In Section 6.5, we introduced the **inverse of a function**. If A and B are nonempty sets and if $f : A \to B$ is a function, then the inverse of f, denoted by f^{-1}, is defined as

$$\begin{aligned} f^{-1} &= \{(b, a) \in B \times A \mid f(a) = b\} \\ &= \{(b, a) \in B \times A \mid (a, b) \in f\}. \end{aligned} \tag{7.1.7}$$

   Now that we know about relations, we see that f^{-1} is always a relation from B to A. The concept of the inverse of a function is actually a special case of the more general concept of the inverse of a relation, which we now define.

   Definition

   Let R be a relation from the set A to the set B. The inverse of R, written R^{-1} and read "R inverse," is the relation from B to A defined by

$$R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}, \text{ or}$$

$$\begin{aligned} R^{-1} &= \{(y,x) \in B \times A \mid (x,y) \in R\}, \text{ or} \\ R^{-1} &= \{(y,x) \in B \times A \mid x \; R \; y\}. \end{aligned} \tag{7.1.8}$$

That is, R^{-1} is the subset of $B \times A$ consisting of all ordered pairs (y,x) such that $x \; R \; y$.

For example, let D be the “divides” relation on $\mathbb{Z}$. See Progress Check 7.3. So

$$D = \{(m,n) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divides } n\}. \tag{7.1.9}$$

This means that we can write $m \mid n$ if and only if $(m,n) \in D$. So, in this case,

$$\begin{aligned} D^{-1} &= \{(n,m) \in \mathbb{Z} \times \mathbb{Z} \mid (m,n) \in D\} \\ &= \{(n,m) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divides } n\}. \end{aligned} \tag{7.1.10}$$

Now, if we would like to focus on the first coordinate instead of the second coordinate in D^{-1}, we know that “m divides n” means the same thing as “n is a multiple of m.” Hence,

$$D^{-1} = \{(n,m) \in \mathbb{Z} \times \mathbb{Z} \mid n \text{ is a multiple of } m\}. \tag{7.1.11}$$

We can say that the inverse of the “divides” relation on $\mathbb{Z}$ is the “is a multiple of” relation on $\mathbb{Z}$.
Theorem 7.6, which follows, contains some elementary facts about inverse.

Theorem 7.6.

Let R be a relation from the set A to the set B. Then

- The domain of R^{-1} is the range of R. That is, dom(R^{-1}) = range(R).
- The range of R^{-1} is the domain of R. That is, range(R^{-1}) = dom(R).
- The inverse of R^{-1} is R. That is, $(R^{-1})^{-1} = R$.

To prove the first part of Theorem 7.6, observe that the goal is to prove that two sets are equal,

$$\text{dom}(R^{-1}) = \text{range}(R)$$

One way to do this is to prove that each is a subset of the other. To prove that dom(R^{-1}) $\subseteq$ range(R), we can start by choosing an arbitrary element of dom(R^{-1}). So let $y \in$ dom(R^{-1}). The goal now is to prove that $y \in$ range(R). What does it mean to say that $y \in$ dom(R^{-1})? It means that there exists an $x \in A$ such that

$$(y,x) \in R^{-1}.$$

Now what does it mean to say that $(y,x) \in R^{-1}$? It means that $(x,y) \in R$. What does this tell us about y?

Complete the proof of the first part of Theorem 7.6. Then, complete the proofs of the other two parts of Theorem 7.6.

Proof

Add proof here and it will automatically be hidden

Answer

Add texts here. Do not delete this text first.

This page titled 7.1: Relations is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

7.2: Equivalence Relations

Preview Activity $7.2.1$: Properties of Relations

In previous mathematics courses, we have worked with the equality relation. For example, let R be the relation on $\mathbb{Z}$ defined as follows: For all $a, b \in \mathbb{Z}$, $a\ R\ b$ if and only if $a = b$. We know this equality relation on $\mathbb{Z}$ has the following properties:

- For each $a \in \mathbb{Z}$, $a = b$ and so $a\ R\ a$.
- For all $a, b \in \mathbb{Z}$, if $a = b$, then $b = a$. That is, if $a\ R\ b$, then $b\ R\ a$.
- For all $a, b, c \in \mathbb{Z}$, if $a = b$ and $b = c$, then $a = c$. That is, if $a\ R\ b$ and $b\ R\ c$, then $a\ R\ c$.

In mathematics, when something satisfies certain properties, we often ask if other things satisfy the same properties. Before investigating this, we will give names to these properties.

Definition

Let A be nonempty set and let R be a relation on A.

- The relation R is **reflexive on** A provided that for each $x \in A$, $x\ R\ x$ or, equivalently, $(x, x) \in R$.
- The relation R is **symmetric** provided that for every $x, y \in A$, if $x\ R\ y$, then $y\ R\ x$ or, equivalently, for every $x, y \in A$, if $(x, y) \in R$, then $(y, x) \in R$.
- The relation R is **transitive** provided that for every $x, y, z \in A$, if $x\ R\ y$ and $y\ R\ z$, then $x\ R\ z$ or, equivalently, for every $x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

Before exploring examples, for each of these properties, it is a good idea to understand what it means to say that a relation does not satisfy the property. So let A be a nonempty set and let R be a relation on A.

1. Carefully explain what it means to say that the relation R is not reflexive on the set A.
2. Carefully explain what it means to say that the relation R is not symmetric.
3. Carefully explain what it means to say that the relation R is not transitive.
   To illustrate these properties, we let $A = \{1, 2, 3, 4\}$ and define the relations R and T on A as follows:

$$\begin{aligned} R &= \{(1,1), (2,2), (3,3), (4,4), (1,3), (3,2)\} \\ T &= \{(1,1), (1,4), (2,4), (4,1), (4,2)\} \end{aligned} \tag{7.2.1}$$

4. Draw a directed graph for the relation R. Then explain why the relation R is reflexive on A, is not symmetric, and is not transitive.
5. Draw a directed graph for the relation T. Is the relation T reflexive on A? Is the relation T symmetric? Is the relation T transitive? Explain.

Preview Activity $7.2.2$: Review of Congruence Modulo n

1. Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. On page 92 of Section 3.1, we defined what it means to say that a is congruent to b modulo n. Write this definition and state two different conditions that are equivalent to the definition.
2. Explain why congruence modulo n is a relation on $\mathbb{Z}$.
3. Carefully review Theorem 3.30 and the proofs given on page 148 of Section 3.5. In terms of the properties of relations introduced in Preview Activity $7.2.1$, what does this theorem say about the relation of congruence modulo non the integers?
4. Write a complete statement of Theorem 3.31 on page 150 and Corollary 3.32.
5. Write a proof of the symmetric property for congruence modulo n. That is, prove the following:

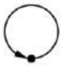
Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. If $a \equiv b$ (mod n), then $b \equiv a$ (mod n).

Directed Graphs and Properties of Relations

In Section 7.1, we used directed graphs, or digraphs, to represent relations on finite sets. Three properties of relations were introduced in Preview Activity $7.2.1$ and will be repeated in the following descriptions of how these properties can be visualized on a directed graph.

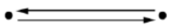
Let A be a nonempty set and let R be a relation on A.

- The relation R is **reflexive on** A provided that for each $x \in A$, $x\ R\ x$ or, equivalently, .$(x,x) \in R$. This means that if a reflexive relation is represented on a digraph, there would have to be a loop at each vertex, as is shown in the following figure.



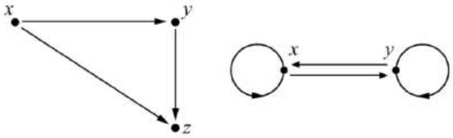
- The relation R is **symmetric** provided that for every $x, y \in A$, if $x\ R\ y$, then $y\ R\ x$ or, equivalently, for every $x, y \in A$, if $(x,y) \in R$, then $(y,x) \in R$.

  This means that if a symmetric relation is represented on a digraph, then anytime there is a directed edge from one vertex to a second vertex, there would be a directed edge from the second vertex to the first vertex, as is shown in the following figure.



- The relation R is **transitive** provided that for every $x, y, z \in A$, if $x\ R\ y$ and $y\ R\ z$, then $x\ R\ z$ or, equivalently, for every $x, y, z \in A$, if $(x,y) \in R$ and $(y,z) \in R$, then $(x,z) \in R$. So if a transitive relation is represented by a digraph, then anytime there is a directed edge from a vertex x to a vertex y and a directed edge from y to a vertex z, there would be a directed edge from x to z.

  In addition, if a transitive relation is represented by a digraph, then anytime there is a directed edge from a vertex x to a vertex y and a directed edge from y to the vertex x, there would be loops at x and y. These two situations are illustrated as follows:



Progress Check 7.7: Properties of Relations

Let $A = \{a, b, c, d\}$ and let R be the following relation on A:

$$R = \{(a,a), (b,b), (a,c), (c,a), (b,d), (d,b)\}.$$

Draw a directed graph for the relation R and then determine if the relation R is reflexive on A, if the relation R is symmetric, and if the relation R is transitive.

Answer

Add texts here. Do not delete this text first.

Definition of an Equivalence Relation

In mathematics, as in real life, it is often convenient to think of two different things as being essentially the same. For example, when you go to a store to buy a cold soft drink, the cans of soft drinks in the cooler are often sorted by brand and type of soft drink. The Coca Colas are grouped together, the Pepsi Colas are grouped together, the Dr. Peppers are grouped together, and so on. When we choose a particular can of one type of soft drink, we are assuming that all the cans are essentially the same. Even though the specific cans of one type of soft drink are physically different, it makes no difference which can we choose. In doing this, we are saying that the cans of one type of soft drink are equivalent, and we are using the mathematical notion of an equivalence relation.

An equivalence relation on a set is a relation with a certain combination of properties that allow us to sort the elements of the set into certain classes. In this section, we will focus on the properties that define an equivalence relation, and in the next section, we will see how these properties allow us to sort or partition the elements of the set into certain classes.

Definition: equivalence relation

Let A be a nonempty set. A relation $\sim$ on the set A is an **equivalence relation** provided that $\sim$ is reflexive, symmetric, and transitive. For $a, b \in A$, if $\sim$ is an equivalence relation on A and $a \sim b$, we say that a **is equivalent to** b.

Most of the examples we have studied so far have involved a relation on a small finite set. For these examples, it was convenient to use a directed graph to represent the relation. It is now time to look at some other type of examples, which may prove to be more interesting. In these examples, keep in mind that there is a subtle difference between the reflexive property and the other two properties. The reflexive property states that some ordered pairs actually belong to the relation R, or some elements of A are related. The reflexive property has a universal quantifier and, hence, we must prove that for all $x \in A$, $x \; R \; x$. Symmetry and transitivity, on the other hand, are defined by conditional sentences. We often use a direct proof for these properties, and so we start by assuming the hypothesis and then showing that the conclusion must follow from the hypothesis.

Example 7.8: A Relation that Is Not an Equivalence Relation

Let M be the relation on $\mathbb{Z}$ defined as follows:

For $a, b \in \mathbb{Z}$, $a \; M \; b$ if and only if a is a multiple of b.

So $a \; M \; b$ if and only if there exists a $k \in \mathbb{Z}$ such that $a = bk$.

- The relation M is reflexive on $\mathbb{Z}$ since for each $x \in \mathbb{Z}$, $x = x \cdot 1$ and, hence, $x \; M \; x$.
- Notice that $4 \; M \; 2$, but $2 \not{M} 4$ So there exist integers x and y such that $x \; M \; y$ but $y \not{M} x$ Hence, the relation M is not symmetric.
- Now assume that $x \; M \; y$ and $y \; M \; z$. Then there exist integers p and q such that

$$x = yp \text{ and } y = zq. \tag{7.2.2}$$

  Using the second equation to make a substitution in the first equation, we see that $x = z(pq)$. Since $pq \in \mathbb{Z}$, we have shown that x is a multiple of z and hence $x \; M \; z$. Therefore, M is a transitive relation.

The relation M is reflexive on $\mathbb{Z}$ and is transitive, but since M is not symmetric, it is not an equivalence relation on $\mathbb{Z}$.

Solution

Add text here.

Progress check 7.9 (a relation that is an equivalence relation)

Define the relation $\sim$ on $\mathbb{Q}$ as follows: For all $a, b \in Q$, $a \sim b$ if and only if $a - b \in \mathbb{Z}$. For example:

- $\frac{3}{4} \sim \frac{7}{4}$ since $\frac{3}{4} - \frac{7}{4} = -1$ and $-1 \in \mathbb{Z}$.
- $\frac{3}{4} \nsim \frac{1}{2}$ since $\frac{3}{4} - \frac{1}{2} = \frac{1}{4}$ and $\frac{1}{4} \notin \mathbb{Z}$.

To prove that $\sim$ is reflexive on $\mathbb{Q}$, we note that for all $q \in \mathbb{Q}$, $a - a = 0$. Since $0 \in \mathbb{Z}$, we conclude that $a \sim a$. Now prove that the relation $\sim$ is symmetric and transitive, and hence, that $\sim$ is an equivalence relation on $\mathbb{Q}$.

Answer

Add texts here. Do not delete this text first.

Congruence Modulo n

One of the important equivalence relations we will study in detail is that of congruence modulo n. We reviewed this relation in Preview Activity $7.2.2$.

Theorem 3.30 tells us that congruence modulo n is an equivalence relation on $\mathbb{Z}$. Recall that by the Division Algorithm, if $a \in \mathbb{Z}$, then there exist unique integers q and r such that

$$a = nq + r \text{ and } 0 \le r < n.$$

Theorem 3.31 and Corollary 3.32 then tell us that $a \equiv r \pmod{n}$. That is, a is congruent modulo n to its remainder r when it is divided by n. When we use the term “remainder” in this context, we always mean the remainder r with $0 \le r < n$ that is guaranteed by the Division Algorithm. We can use this idea to prove the following theorem.

Theorem 7.10

Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n.

Proof

Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. We will first prove that if a and b have the same remainder when divided by n, then $a \equiv b$ (mod n). So assume that a and bhave the same remainder when divided by n, and let r be this common remainder. Then, by Theorem 3.31,

$$a \equiv r \pmod{n} \text{ and } b \equiv r \pmod{n}.$$

Since congruence modulo n is an equivalence relation, it is a symmetric relation. Hence, since $b \equiv r \pmod{n}$, we can conclude that $r \equiv b \pmod{n}$. Combining this with the fact that $a \equiv r \pmod{n}$, we now have

$$a \equiv r \pmod{n} \text{ and } r \equiv b \pmod{n}$$

We can now use the transitive property to conclude that $a \equiv b \pmod{n}$. This proves that if a and b have the same remainder when divided by n, then $a \equiv b \pmod{n}$.

We will now prove that if $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n. Assume that $a \equiv b$ (mod n), and let r be the least nonnegative remainder when b is divided by n. Then $0 \le r < n$ and, by Theorem 3.31,

$$b \equiv r \pmod{n}.$$

Now, using the facts that $a \equiv b \pmod{n}$ and $b \equiv r \pmod{n}$, we can use the transitive property to conclude that

$$a \equiv r \pmod{n}$$

This means that there exists an integer q such that $a - r = nq$ or that

$a = nq + r.$

Since we already know that $0 \le r < n$, the last equation tells us that r is the least nonnegative remainder when a is divided by n. Hence we have proven that if $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n.

Examples of Other Equivalence Relations

1. The relation $\sim$ on $\mathbb{Q}$ from Progress Check 7.9 is an equivalence relation.
2. Let A be a nonempty set. The **equality relation on** A is an equivalence relation. This relation is also called the **identity relation on** A and is denoted by I_A, where

$$I_A = \{(x, x) \mid x \in A\}. \tag{7.2.3}$$

3. Define the relation $\sim$ on $\mathbb{R}$ as follows:
For $a, b \in \mathbb{R}$, $a \sim b$ if and only if there exists an integer k such that $a - b = 2k\pi$.

We will prove that the relation ~ is an equivalence relation on $\mathbb{R}$. The relation $\sim$ is reflexive on $\mathbb{R}$ since for each $a \in \mathbb{R}$, $a - a = 0 = 2 \cdot 0 \cdot \pi$.
Now, let $a, b \in \mathbb{R}$ and assume that $a \sim b$. We will prove that $b \sim a$. Since $a \sim b$, there exists an integer k such that

$$a - b = 2k\pi. \tag{7.2.4}$$

By multiplying both side of this equation by -1, we obtain

$$\begin{aligned} (-1)(a-b) &= (-1)(2k\pi) \\ b - a &= 2(-k)\pi. \end{aligned} \tag{7.2.5}$$

Since $-k \in \mathbb{Z}$, the last equation proves that $b \sim a$. Hence, we have proven that if $a \sim b$, then $b \sim a$ and, therefore, the relation $\sim$ is symmetric.

To prove transitivity, let $a, b, c \in \mathbb{R}$ and assume that $a \sim b$ and $b \sim c$. We will prove that $a \sim c$. Now, there exist integers k and n such that

$$a - b = 2k\pi \text{ and } b - c = 2n\pi. \tag{7.2.6}$$

By adding the corresponding sides of these two equations, we see that

$$\begin{aligned} (a-b)+(b-c) &= 2k\pi + 2n\pi \\ a - c &= 2(k+n)\pi. \end{aligned} \tag{7.2.7}$$

By the closure properties of the integers, $k + n \in \mathbb{Z}$. So this proves that $a \sim c$ and, hence the relation $\sim$ is transitive.

We have now proven that $\sim$ is an equivalence relation on $\mathbb{R}$. This equivalence relation is important in trigonometry. If $a \sim b$, then there exists an integer k such that $a - b = 2k\pi$ and, hence, $a = b + k(2\pi)$. Since the sine and cosine functions are periodic with a period of 2π, we see that

$$\begin{aligned} sin\ a &= sin(b + k(2\pi)) = sin\ b, \text{ and} \\ cos\ a &= cos(b + k(2\pi)) = cos\ b. \end{aligned} \tag{7.2.8}$$

Therefore, when $a \sim b$, each of the trigonometric functions have the same value at a and b.

4. For an example from Euclidean geometry, we define a relation P on the set $\mathcal{L}$ of all lines in the plane as follows:

   For$l_1, l_2 \in \mathcal{L}$, $l_1 \; P \; l_2$ if and only if l_1 is parallel to l_2 or $l_1 = l_2$.

   We added the second condition to the definition of P to ensure that P is reflexive on $\mathcal{L}$. Theorems from Euclidean geometry tell us that if l_1 is parallel to l_2, then l_2 is parallel to l_1, and if l_1 is parallel to l_2 and l_2 is parallel to l_3, then l_1 is parallel to l_3. (Drawing pictures will help visualize these properties.) This tells us that the relation P is reflexive, symmetric, and transitive and, hence, an equivalence relation on $\mathcal{L}$.

? Progress Check 7.11: Another Equivalence Relation

Let U be a finite, nonempty set and let $\mathcal{P}(U)$ be the power set of U. Recall that $\mathcal{P}(U)$ consists of all subsets of U. (See page 222.) Define the relation $\approx$ on $\mathcal{P}(U)$ as follows:

For $A, B \in P(U)$, $A \approx B$ if and only if card(A) = card(B).

For the definition of the cardinality of a finite set, see page 223. This relation states that two subsets of U are equivalent provided that they have the same number of elements. Prove that $\approx$ is an equivalence relation on

Answer

Add texts here. Do not delete this text first.

? Exercise 7.2

1. Let $A = \{a, b\}$ and let $R = \{(a, b)\}$. Is R an equivalence relation on A? If not, is R reflexive, symmetric, or transitive? Justify all conclusions.
2. Let $A = \{a, b, c\}$. For each of the following, draw a directed graph that represents a relation with the specified properties.

   (a) A relation on A that is symmetric but not transitive
   (b) A relation on A that is transitive but not symmetric
   (c) A relation on A that is symmetric and transitive but not reflexive on A

(d) A relation on A that is not reflexive on A, is not symmetric, and is not transitive
(e) A relation on A, other than the identity relation, that is an equivalence relation on A

3. Let $A = \{1, 2, 3, 4, 5\}$. The identity relation on A is

$$I_A = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)\}. \tag{7.2.9}$$

Determine an equivalence relation on A that is different from I_A or explain why this is not possible.

4. Let $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid |x| + |y| = 4\}$. Then R is a relation on $\mathbb{R}$. Is R an equivalence relation on $\mathbb{R}$? If not, is R reflexive, symmetric, or transitive? Justify all conclusions.
5. A relation R is defined on $\mathbb{Z}$ as follows: For all a, b in $\mathbb{Z}$, $a\ R\ b$ if and only if $|a - b| \le 3$. Is R an equivalence relation on $\mathbb{R}$? If not, is R reflexive, symmetric, or transitive. Justify all conclusions.
6. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 - 4$ for each $x \in \mathbb{R}$. Define a relation $\sim$ on $\mathbb{R}$ as follows:
For $a, b \in \mathbb{R}$, $a \sim b$ if and only if $f(a) = f(b)$.
(a) Is the relation an equivalence relation on $\mathbb{R}$?Justify your conclusion.
(b) Determine all real numbers in the set $C = \{x \in R \mid x \sim 5\}$.
7. Repeat Exercise (6) using the function $f : \mathbb{R} \to \mathbb{R}$ that is defined by $f(x) = x^2 - 3x - 7$ for each $x \in \mathbb{R}$.
8. (a) Repeat Exercise (6a) using the function $f : \mathbb{R} \to \mathbb{R}$ that is defined by $f(x) = sin\ x$ for each $x \in \mathbb{R}$.
(b) Determine all real numbers in the set $C = \{x \in \mathbb{R} \mid x \sim \pi\}$.
9. Define the relation $\sim$ on $\mathbb{Q}$ as follows: For $a, b \in \mathbb{Q}$, $a \sim b$ if and only if $a - b \in \mathbb{Z}$. In progress Check 7.9, we showed that the relation $\sim$ is a equivalence relation on $\mathbb{Q}$.

(a) List four different elements of the set $C = \{x \in \mathbb{Q} \mid x \sim \dfrac{5}{7}\}$.
(b) Use set builder notation (without using the symbol sim) to specify the set C.
(c) Use the roster method to specify the set C.

10. Let $\sim$ and $\approx$ be relation on $\mathbb{Z}$ defined as follows:

- For $a, b \in Z$, $a \sim b$ if and only if 2 divides $a + b$.
- For $a, b \in Z$, $a \approx b$ if and only if 3 divides $a + b$.

(a) Is $\sim$ an equivalence relation on $\mathbb{Z}$? If not, is this relation reflexive, symmetric, or transitive?
(b)Is $\approx$ an equivalence relation on $\mathbb{Z}$? If not, is this relation reflexive, symmetric, or transitive?

11. Let U be a finite, nonempty set and let $\mathcal{P}(U)$ be the power set of U. That is, $\mathcal{P}(U)$ is the set of all subsets of U. Define the relation $\sim$ on $\mathcal{P}(U)$ as follows: For $A, B \in P(U)$, $A \sim B$ if and only if $A \cap B = \emptyset$. That is, the ordered pair (A, B) is in the relaiton $\sim$ if and only if A and B are disjoint.
Is the relation $\sim$ an equivalence relation on $\mathcal{P}(U)$? If not, is it reflexive, symmetric, or transitive? Justify all conclusions.
12. Let U be a nonempty set and let $\mathcal{P}(U)$ be the power set of U. That is, $\mathcal{P}(U)$ is the set of all subsets of U.
For A and B in $\mathcal{P}(U)$, define $A \sim B$ to mean that there exists a bijection $f : A \to B$. Prove that $\sim$ is an equivalence relation on $\mathcal{P}(U)$.
Hint: Use results from Sections 6.4 and 6.5.
13. Let $\sim$ and $\approx$ be relation on $\mathbb{Z}$ defined as follows:

- For $a, b \in Z$, $a \sim b$ if and only if $2a + 3b \equiv 0$ (mod 5).
- For $a, b \in Z$, $a \approx b$ if and only if $a + 3b \equiv 0$ (mod 5).

(a) Is $\sim$ an equivalence relation on $\mathbb{Z}$? If not, is this relation reflexive, symmetric, or transitive?
(b)Is $\approx$ an equivalence relation on $\mathbb{Z}$? If not, is this relation reflexive, symmetric, or transitive?

14. Let $\sim$ and $\approx$ be relation on $\mathbb{R}$ defined as follows:

- For $a, b \in Z$, $a \sim b$ if and only if $xy \ge 0$.
- For $a, b \in Z$, $a \approx b$ if and only if $xy \le 0$.

(a) Is $\sim$ an equivalence relation on $\mathbb{R}$? If not, is this relation reflexive, symmetric, or transitive?
(b)Is $\approx$ an equivalence relation on $\mathbb{R}$? If not, is this relation reflexive, symmetric, or transitive?

15. Define the relation $\approx$ on $\mathbb{R} \times \mathbb{R}$ as follows: For $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$, $(a, b) \approx (c, d)$ if and only if $a^2 + b^2 = c^2 + d^2$.

(a) Prove that $\approx$ is an equivalence relation on $\mathbb{R} \times \mathbb{R}$.
(b) List four different elements of the set

$$C = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid (x, y) \approx (4, 3)\}. \tag{7.2.10}$$

(c) Give a geometric description of set C.

16. **Evaluation of proofs**
See the instructions for Exercise (19) on page 100 from Section 3.1.

(a)

Proposition. Let R be a relation on a set A. If R is symmetric and transitive, then R is reflexive.

Proof

Let $x, y \in A$. If $x\ R\ y$, then $y\ R\ x$ since R is symmetric. Now, $x\ R\ y$ and $y\ R\ x$, and since R is transitive, we can conclude that $x\ R\ x$. Therefore, R is reflexive.

(b)

Proposition. Let $\sim$ be a relation on $\mathbb{Z}$ where for all $a, b \in \mathbb{Z}$, $a \sim b$ if and only if $(a + 2b) \equiv 0$ (mod 3). The relation $\sim$ is an equivalence relation on $\mathbb{Z}$.

Proof

Assume $a \sim a$. Then $(a + 2a) \equiv 0$ (mod 3) since $(3a) \equiv 0$ (mod 3). Therefore, $\sim$ is reflexive on $\mathbb{Z}$. In addition, if $a \sim b$, then $(a + 2b) \equiv 0$ (mod 3), and if we multiply both sides of this congruence by 2, we get

$$\begin{aligned} 2(a+2b) &\equiv 2 \cdot 0 \pmod 3 \\ (2a+4b) &\equiv 0 \pmod 3 \\ (a+2b) &\equiv 0 \pmod 3 \\ (b+2a) &\equiv 0 \pmod 3. \end{aligned} \tag{7.2.11}$$

This means that $b \sim a$ and hence, $\sim$ is symmetric.

We now assume that $(a + 2b) \equiv 0$ (mod 3) and $(b + 2c) \equiv 0$ (mod 3).

By adding the corresponding sides of these two congruences, we obtain

$$\begin{aligned} (a+2b)+(b+2c) &\equiv 0+0 \pmod 3 \\ (a+3b+2c) &\equiv 0 \pmod 3 \\ (a+2c) &\equiv 0 \pmod 3. \end{aligned} \tag{7.2.12}$$

Hence, the relation $\sim$ is transitive and we have proved that $\sim$ is an equivalence relation on $\mathbb{Z}$.

Explorations and Activities

17. **Other Types of Relations.** In this section, we focused on the properties of a relation that are part of the definition of an equivalence relation. However, there are other properties of relations that are of importance. We will study two of these properties in this activity.

A relation R on a set A is a circular relation provided that for all x, y, and z in A, if $x\ R\ y$ and $y\ R\ z$, then $z\ R\ x$.

(a) Carefully explain what it means to say that a relation R on a set A is not circular.

(b) Let $A = \{1, 2, 3\}$. Draw a directed graph of a relation on A that is circular and draw a directed graph of a relation on A that is not circular.
(c) Let $A = \{1, 2, 3\}$. Draw a directed graph of a relation on A that is circular and not transitive and draw a directed graph of a relation on A that is transitive and not circular.

(d) Prove the following proposition:
A relation R on a set A is an equivalence relation if and only if it is reflexive and circular.

A relation R on a set A is an **antisymmetric relation** provided that for all $x, y \in A$, if $x\ R\ y$ and $y\ R\ x$, then $x = y$.

(e) Carefully explain what it means to say that a relation on a set A is not antisymmetric.

(f) Let $A = \{1, 2, 3\}$. Draw a directed graph of a relation on A that is antisymmetric and draw a directed graph of a relation on A that is not antisymmetric.

(g)Are the following propositions true or false? Justify all conclusions.

- If a relation R on a set A is both symmetric and antisymmetric, then R is transitive.
- If a relation R on a set A is both symmetric and antisymmetric, then R is reflexive.

Answer

Add texts here. Do not delete this text first.

This page titled 7.2: Equivalence Relations is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

7.3: Equivalence Classes

PREVIEW ACTIVITY $7.3.1$: Sets Associated with a Relation

As was indicated in Section 7.2, an equivalence relation on a set A is a relation with a certain combination of properties (reflexive, symmetric, and transitive) that allow us to sort the elements of the set into certain classes. This is done by means of certain subsets of A that are associated with the elements of the set A. This will be illustrated with the following example. Let $A = \{a, b, c, d, e\}$, and let R be the relation on the set A defined as follows:

$a\ R\ a\ \ b\ R\ b\ \ c\ R\ c\ \ d\ R\ d\ \ e\ R\ e$
$a\ R\ b\ \ b\ R\ a\ \ b\ R\ e\ \ e\ R\ b$
$a\ R\ e\ \ e\ R\ a\ \ c\ R\ d\ \ d\ R\ c$

For each $y \in A$, define the subset $R[y]$ of A as follows:

$$R[y] = \{x \in A \mid x\ R\ y\}.$$

That is, $R[y]$ consists of those elements in A such that $x\ R\ y$. For example, using $y = a$, we see that $a\ R\ a$, $b\ R\ a$, and $e\ R\ a$, and so $R[a] = \{a, b, e\}$.

1. Determine $R[b]$, $R[c]$, $R[d]$ and $R[e]$.
2. Draw a directed graph for the relation R and explain why R is an equivalence relation on A.
3. Which of the sets $R[a]$, $R[b]$, $R[c]$, $R[d]$ and $R[e]$ are equal?
4. Which of the sets $R[a]$, $R[b]$, $R[c]$, $R[d]$ and $R[e]$ are disjoint?

As we will see in this section, the relationships between these sets is typical for an equivalence relation. The following example will show how different this can be for a relation that is not an equivalence relation.

Let $A = \{a, b, c, d\}$, and let S be the relation on the set A defined as follows:

$b\ S\ b\ \ c\ S\ c\ \ d\ S\ d\ \ e\ S\ e$
$a\ S\ b\ \ a\ S\ d\ \ b\ S\ c$
$c\ S\ d\ \ d\ S\ c$

5. Draw a digraph that represents the relation S on A. Explain why S is not an equivalence relation on A.

For each $y \in A$, define the subset $S[y]$ of A as follows:
$$S[y] = \{x \in A \mid x\ S\ y\} = \{x \in A \mid (x, y) \in S\}.$$

For example, using $y = b$, we see that $S[b] = \{a, b\}$ since $(a, b) \in S$ and $(b, b) \in S$. In addition, we see that $S[a] = \emptyset$ since there is no x 2 A such that.x;a/ 2 S.

6. Determine $S[c]$, $S[d]$, and $S[e]$.

7. Which of the sets $S[a]$, $S[b]$, $S[c]$, $S[d]$, and $S[e]$ are equal?

8. Which of the sets $S[b]$, $S[c]$, $S[d]$, and $S[e]$ are disjoint?

PREVIEW ACTIVITY $7.3.2$: Congruence Modulo 3

An important equivalence relation that we have studied is congruence modulo n on the integers. We can also define subsets of the integers based on congruence modulo n. We will illustrate this with congruence modulo 3. For example, we can define $C[0]$ to be the set of all integers a that are congruent to 0 modulo 3. That is,

$$C[0] = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 3\}.$$

Since an integer a is congruent to 0 modulo 3 if an only if 3 divides a, we can use the roster method to specify this set as follows:

$$C[0] = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}.$$

1. Use the roster method to specify each of the following sets:

   (a) The set $C[1]$ of all integers a that are congruent to 1 modulo 3. That is, $C[1] = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 3\}$.
   (b) The set $C[2]$ of all integers a that are congruent to 2 modulo 3. That is, $C[2] = \{a \in \mathbb{Z} \mid a \equiv 2 \pmod 3\}$.
   (c) The set $C[3]$ of all integers a that are congruent to 3 modulo 3. That is, $C[3] = \{a \in \mathbb{Z} \mid a \equiv 3 \pmod 3\}$.
2. Now consider the three sets, $C[0]$, $C[1]$, and $C[2]$.

   (a) Determine the intersection of any two of these sets. That is, determine $C[0] \cap C[1]$, $C[0] \cap C[2]$, and $C[1] \cap C[2]$.
   (b) Let $n = 734$. What is the remainder when n is divided by 3? Which of the three sets, if any, contains $n = 734$?
   (c) Repeat Part (2b) for $n = 79$ and for $n = -79$.
   (d) Do you think that $C[0] \cup C[1] \cup C[2] = \mathbb{Z}$ Explain.
   (e) Is the set $C[3]$ equal to one of the sets $C[0]$, $C[1]$, or $C[2]$?
   (f) We can also define $C[4] = \{a \in \mathbb{Z} \mid a \equiv 4 \pmod 3\}$. Is this set equal to any of the previous sets we have studied in this part? Explain.

The Definition of an Equivalence Class

We have indicated that an equivalence relation on a set is a relation with a certain combination of properties (reflexive, symmetric, and transitive) that allow us to sort the elements of the set into certain classes. We saw this happen in the preview activities. We can now illustrate specifically what this means. For example, in Preview Activity $7.3.2$, we used the equivalence relation of congruence modulo 3 on $\mathbb{Z}$ to construct the following three sets:

$$\begin{aligned} C[0] &= \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 3\}, \\ C[1] &= \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 3\}, \text{ and} \\ C[2] &= \{a \in \mathbb{Z} \mid a \equiv 2 \pmod 3\}. \end{aligned} \tag{7.3.1}$$

The main results that we want to use now are Theorem 3.31 and Corollary 3.32 on page 150. This corollary tells us that for any $a \in \mathbb{Z}$, a is congruent to precisely one of the integers 0, 1, or 2. Consequently, the integer a must be congruent to 0, 1, or 2, and it cannot be congruent to two of these numbers. Thus

1. For each $a \in \mathbb{Z}$, $a \in C[0]$, $a \in C[1]$, or $a \in C[2]$; and
2. $C[0] \cap C[1] = \emptyset$, $C[0] \cap C[2] = \emptyset$, and $C[1] \cap C[2] = \emptyset$.

This means that the relation of congruence modulo 3 sorts the integers into three distinct sets, or classes, and that each pair of these sets have no elements in common. So if we use a rectangle to represent $\mathbb{Z}$, we can divide that rectangle into three smaller rectangles, corresponding to $C[0]$, $C[1]$, and $C[2]$ and we might picture this situation as follows:

The Integers

$C[0]$ consisting of all integers with a remainder of 0 when divided by 3	$C[1]$ consisting of all integers with a remainder of 1 when divided by 3	$C[2]$ consisting of all integers with a remainder of 2 when divided by 3

Each integer is in exactly one of the three sets (C[0]\), $C[1]$, or $C[2]$, and two integers are congruent modulo 3 if and only if they are in the same set. We will see that, in a similar manner, if n is any natural number, then the relation of congruence modulo n can be used to sort the integers into n classes. We will also see that in general, if we have an equivalence relation R on a set A, we can sort the elements of the set A into classes in a similar manner.

Definition

Let $\sim$ be an equivalence relation on a nonempty set A. For each $a \in A$, the equivalence class of a determined by $\sim$ is the subset of A, denoted by $[a]$, consisting of all the elements of A that are equivalent to a. That is,

$$[a] = \{x \in A \mid x \sim a\}.$$

We read $[a]$ as "the equivalence class of a" or as "bracket a."

Notes

1. We use the notation $[a]$ when only one equivalence relation is being used. If there is more than one equivalence relation, then we need to distinguish between the equivalence classes for each relation. We often use something like $[a]_\sim$, or if R is the name of the relation, we can use $R[a]$ or $[a]_R$ for the equivalence class of a determined by R. In any case, always remember that when we are working with any equivalence relation on a set A if $a \in A$, then *the equivalence class* $[a]$ *is a subset of* A.
2. We know that each integer has an equivalence class for the equivalence relation of congruence modulo 3. But as we have seen, there are really only three distinct equivalence classes. Using the notation from the definition, they are:

$[0] = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 3\}$,
$[1] = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 3\}$, and
$[2] = \{a \in \mathbb{Z} \mid a \equiv 2 \pmod 3\}$.

Progress Check 7.12 (Equivalence Classes from Preview Activity 7.3.1)

Without using the terminology at that time, we actually determined the equivalence classes of the equivalence relation R in Preview Activity 7.3.1. What are the distinct equivalence classes for this equivalence relation?

Answer

Add texts here. Do not delete this text first.

Congruence Modulo n and Congruence Classes

In Preview Activity 7.3.2, we used the notation $C[k]$ for the set of all integers that are congruent to k modulo 3. We could have used a similar notation for equivalence classes, and this would have been perfectly acceptable. However, the notation $[a]$ is probably the most common notation for the equivalence class of a. We will now use this same notation when dealing with congruence modulo n when only one congruence relation is under consideration.

Definition: congruence class of a modulo n.

Let $n \in \mathbb{N}$. Congruence modulo n is an equivalence relation on $\mathbb{Z}$. So for $a \in \mathbb{Z}$,

$$[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod n\}.$$

In this case, $[a]$ is called the **congruence class of a modulo n**.

We have seen that congruence modulo 3 divides the integers into three distinct congruence classes. Each congruence class consists of those integers with the same remainder when divided by 3. In a similar manner, if we use congruence modulo 2, we simply divide the integers into two classes. One class will consist of all the integers that have a remainder of 0 when divided by 2, and the other class will consist of all the integers that have a remainder of 1 when divided by 2. That is, congruence modulo 2 simply divides the integers into the even and odd integers.

Progress Check 7.13: Congruence Modulo 4

Determine all of the distinct congruence classes for the equivalence relation of congruence modulo 4 on the integers. Specify each congruence class using the roster method.

Answer

Add texts here. Do not delete this text first.

Properties of Equivalence Classes

As we have seen, in Preview Activity 7.3.1, the relation R was an equivalence relation. For that preview activity, we used $R[y]$ to denote the equivalence class of $y \in A$, and we observed that these equivalence classes were either equal or disjoint.

However, in Preview Activity 7.3.1, the relation S was not an equivalence relation, and hence we do not use the term “equivalence class” for this relation. We should note, however, that the sets $S[y]$ were not equal and were not disjoint. This exhibits one of the main distinctions between equivalence relations and relations that are not equivalence relations.

In Theorem 7.14, we will prove that if $\sim$ is an equivalence relation on the set A, then we can “sort” the elements of A into distinct equivalence classes. The properties of equivalence classes that we will prove are as follows: (1) Every element of A is in its own equivalence class; (2) two elements are equivalent if and only if their equivalence classes are equal; and (3) two equivalence classes are either identical or they are disjoint.

Theorem 7.14

Let A be a nonempty set and let $\sim$ be an equivalence relation on the set A. Then,

1. For each $a \in A$, $a \in [a]$.
2. For each $a, b \in A$, $a \sim b$ if and only if $[a] = [b]$,
3. For each $a, b \in A$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

Proof

Let A be a nonempty set and assume that $\sim$ is an equivalence relation on A. To prove the first part of the theorem, let $a \in A$. Since $\sim$ is an equivalence relation on A, it is reflexive on A. Thus, $a \sim a$, and we can conclude that $a \in [a]$.

The second part of this theorem is a biconditional statement. We will prove it by proving two conditional statements. We will first prove that if $a \sim b$, then $[a] = [b]$. So let $a, b \in A$ and assume that $a \sim b$. We will now prove that the two sets $[a]$ and $[b]$ are equal. We will do this by proving that each is a subset of the other.

First, assume that $x \in [a]$. Then, by definition, $x \sim a$. Since we have assumed that $a \sim b$, we can use the transitive property of $\sim$ to conclude that $x \sim b$, and this means that $x \in [b]$. This proves that $[a] \subseteq [b]$.

We now assume that $y \in [b]$. This means that $y \sim b$, and hence by the symmetric property, that $b \sim y$. Again, we are assuming that $a \sim b$. So we have

$$a \sim b \text{ and } b \sim y.$$

We use the transitive property to conclude that $a \sim y$ and then, using the symmetric property, we conclude that $y \sim a$. This proves that $y \in [a]$ and, hence, that $[b] \subseteq [a]$. This means that we can conclude that if $a \sim b$, then $[a] = [b]$.

We must now prove that if $[a] = [b]$, then $a \sim b$. Let $a, b \in A$ and assume that $[a] = [b]$. Using the first part of the theorem, we know that $a \in [a]$ and since the two sets are equal, this tells us that $a \in [b]$. Hence by the definition of $[b]$, we conclude that $a \sim b$. This completes the proof of the second part of the theorem.

For the third part of the theorem, let $a, b \in A$. Since this part of the theorem is a disjunction, we will consider two cases: Either

$$[a] \cap [b] = \emptyset \text{ or } [a] \cap [b] \neq \emptyset.$$

In the case where $[a] \cap [b] = \emptyset$, the first part of the disjunction is true, and hence there is nothing to prove. So we assume that $[a] \cap [b] \neq \emptyset$; and will show that $[a] = [b]$. Since $[a] \cap [b] \neq \emptyset$, there is an element x in A such that

$$a \in [a] \cap [b].$$

This means that $x \in [a]$ and $x \in [b]$. Consequently, $x \in a$ and $x \in b$, and so we can use the first part of the theorem to conclude that $[x] = [a]$ and $[x] = [b]$. Hence, $[a] = [b]$, and we have proven that $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

Theorem 7.14 gives the primary properties of equivalence classes. Consequences of these properties will be explored in the exercises. The following table restates the properties in Theorem 7.14 and gives a verbal description of each one.

Formal Statement from Theorem 7.14	Verbal Description
For each $a \in A$, $a \in [a]$.	Every element of A is in its own equivalence class.
For each $a, b \in A$, $a \sim b$ if and only if $[a] = [b]$.	Two elements of A are equivalent if and only if their equivalence classes are equal.
For each $a, b \in A$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$	Any two equivalence classes are either equal or they are disjoint. This means that if two equivalence classes are not disjoint then they must be equal.

Progress Check 7.15: Equivalence Classes

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 - 4$ for each $x \in \mathbb{R}$. Define a relation $\sim$ on $\mathbb{R}$ as follows:

For $a, b \in \mathbb{R}$, $a \sim b$ if and only if $f(a) = f(b)$.

In Exercise (6) of Section 7.2, we proved that $\sim$ is an equivalence relation on $\mathbb{R}$. Consequently, each real number has an equivalence class. For this equivalence relation,

1. Determine the equivalence classes of 5, -5, 10, -10, π, and $-\pi$.
2. Determine the equivalence class of 0.
3. If $a \in \mathbb{R}$, use the roster method to specify the elements of the equivalence class $[a]$.

Answer

Add texts here. Do not delete this text first.

The results of Theorem 7.14 are consistent with all the equivalence relations studied in the preview activities and in the progress checks. Since this theorem applies to all equivalence relations, it applies to the relation of congruence modulo n on the integers. Because of the importance of this equivalence relation, these results for congruence modulo n are given in the following corollary.

Corollary 7.16.

Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, let $[a]$ represent the congruence class of a modulo n.

1. For each $a \in \mathbb{Z}$, $a \in [a]$.
2. For each $a, b \in \mathbb{Z}$, $a \equiv b$ (mod n) if and only if $[a] = [b]$.
3. For each $a, b \in \mathbb{Z}$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

For the equivalence relation of congruence modulo n, Theorem 3.31 and Corollary 3.32 tell us that each integer is congruent to its remainder when divided by n, and that each integer is congruent modulo n to precisely one of one of the integers $0, 1, 2, ..., n - 1$. This means that each integer is in precisely one of the congruence classes $[0], [1], [2], ..., [n - 1]$. Hence, Corollary 7.16 gives us the following result

Theorem 7.3.1

Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, let $[a]$ represent the congruence class of a modulo n.

1. $\mathbb{Z} = [0] \cup [1] \cup [2] \cup \cdots \cup [n - 1]$
2. For $j, k \in \{0, 1, 2, ..., n - 1\}$, if $j \neq k$, then $[j] \cap [k] = \emptyset$.

Partitions and Equivalence Relations

A partition of a set A is a collection of subsets of A that “breaks up” the set A into disjoint subsets. Technically, each pair of distinct subsets in the collection must be disjoint. We then say that the collection of subsets is **pairwise disjoint.** We introduce the following formal definition.

Definition: partition of A

Let A be a nonempty set, and let $\mathcal{C}$ be a collection of subsets of A. The collection of subsets $\mathcal{C}$ is a **partition of** A provided that

1. For each $V \in \mathcal{C}$, $V \neq \emptyset$.
2. For each $x \in A$, there exists a $V \in \mathcal{C}$ such that $x \in V$.
3. For every $V, W \in \mathcal{C}$, $V = W$ or $V \cap W = \emptyset$.

There is a close relation between partitions and equivalence classes since the equivalence classes of an equivalence relation form a partition of the underlying set, as will be proven in Theorem 7.18. The proof of this theorem relies on the results in Theorem 7.14.

Theorem 7.18

Let $\sim$ be an equivalence relation on the nonempty set A. Then the collection $\mathcal{C}$ of all equivalence classes determined by $\sim$ is a partition of the set A.

Proof

Let $\sim$ be an equivalence relation on the nonempty set A, and let $\mathcal{C}$ be the collection of all equivalence classes determined by $\sim$. That is,

$$\mathcal{C} = \{[a] \mid a \in A\}.$$

We will use Theorem 7.14 to prove that $\mathcal{C}$ is a partition of A.

Part (1) of Theorem 7.14 states that for each $a \in A$, $a \in [a]$. In terms of the equivalence classes, this means that each equivalence class is nonempty since each element of A is in its own equivalence class. Consequently, $\mathcal{C}$, the collection of all equivalence classes determined by $\sim$, satisfies the first two conditions of the definition of a partition.

We must now show that the collection $\mathcal{C}$ of all equivalence classes determined by $\sim$ satisfies the third condition for being a partition. That is, we need to show that any two equivalence classes are either equal or are disjoint. However, this is exactly the result in Part (3) of Theorem 7.14.

Hence, we have proven that the collection C of all equivalence classes determined by $\sim$ is a partition of the set A.

Note: Theorem 7.18 has shown us that if $\sim$ is an equivalence relation on a nonempty set A, then the collection of the equivalence classes determined by $\sim$ form a partition of the set A.

This process can be reversed. This means that given a partition $\mathcal{C}$ of a nonempty set A, we can define an equivalence relation on A whose equivalence classes are precisely the subsets of A that form the partition. This will be explored in Exercise (12).

Exercise 7.3

1. Let $A = \{a, b, c, d, e\}$ and let $\sim$ be the relation on A that is represented by the directed graph in Figure 7.4.

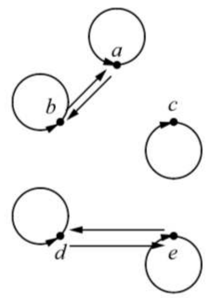


Figure 7.4: Directed Graph for the Relation in Exercise (1)

Prove that $\sim$ is an equivalence relation on the set A, and determine all of the equivalence classes determined by this equivalence relation.

2. Let $A = \{a, b, c, d, e, f\}$, and assume that $\sim$ is an equivalence relation on A. Also assume that it is known that
$a \sim b$ $a \nsim c$ $e \sim f$
$a \sim d$ $a \nsim f$ $e \nsim c$
Draw a complete directed graph for the equivalence relation $\sim$ on the set A, and then determine all of the equivalence classes for this equivalence relation.
3. Let $A = \{0, 1, 2, 3, ..., 999, 1000\}$. Define the relation R on A as follws:
For $x, y \in A$, $x \; R \; y$ if and only if x and y have the same number of digits.

Prove that R is an equivalence relation on the set A and determine all of the distinct equivalence classes determined by R.

4. Determine all of the congruence classes for the relation of congruence modulo 5 on the set of integers.

5. Let $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.
   (a) Define the relation $\sim$ on $\mathbb{Z}_9$ as follows: for all $a, b \in \mathbb{Z}_9$, $a \sim b$ if and only if $a^2 \equiv b^2$ (mod 9). Prove that $\sim$ is an equivalence relation on $\mathbb{Z}_9$ and determine all of the distinct equivalence classes of this equivalence relation.
   (b) Define the relation $\approx$ on $\mathbb{Z}_9$ as follows: For all $a, b \in \mathbb{Z}_9$, $a \approx b$ if and only if $a^3 \equiv b^3$ (mod 9). Prove that $\approx$ is an equivalence relation on $\mathbb{Z}_9$ and determine all of the distinct equivalence classes of this equivalence relation.
6. Define the relation $\sim$ on $\mathbb{Q}$ as follows: For $a, b \in \mathbb{Q}$, $a \sim b$ if and only if $a - b \in \mathbb{Z}$. In Progress Check 7.9 of Section 7.2, we showed that the relation $\sim$ is an equivalence relation on $\mathbb{Q}$. Also, see Exercise (9) in Section 7.2.

   (a) Prove that $[\frac{5}{7} = \{m + \frac{5}{7} \mid m \in \mathbb{Z}\}$.
   (b) If $a \in \mathbb{Z}$, then what is the equivalence class of a?
   (c) If $a \in \mathbb{Z}$, prove that there is a bijection from $[a]$ to $[\frac{5}{7}]$.
7. Define the relation $\sim$ on $\mathbb{R}$ as follows:
   For $x, y \in \mathbb{R}$, $x \sim y$ if and only if $x - y \in \mathbb{Q}$.

   (a) Prove that $\sim$ is an equivalence relation on $\mathbb{R}$.
   (b) List four different real numbers that are in the equivalence class of $\sqrt{2}$.
   (c) If $a \in \mathbb{Q}$, what is the equivalence class of a?
   (d) Prove that $[\sqrt{2}] = \{r + \sqrt{2} \mid r \in \mathbb{Q}\}$.
   (e) If $a \in \mathbb{Q}$, prove that there is a bijection from $[a]$ to $[\sqrt{2}]$.
8. Define the relation $\sim$ on $\mathbb{Z}$ as follows: For $a, b \in \mathbb{Z}$, $a \sim b$ if and only if $(2a + 3b \equiv 0$ (mod 5). The relation $\sim$ is an equivalence relation on $\mathbb{Z}$. (See Exercise (13) in Section 7.2). Determine all the distinct equivalence classes for this equivalence relation.
9. Let $A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$. That is, $A = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \neq 0\}$. Define the relation $\approx$ on A as follows:
   For $(a, b), (c, d) \in A$, $(a, b) \approx (c, d)$ if and only if $ad = bc$.

   (a) Prove that $\approx$ is an equivalence relation on A.
   (b) Why was it necessary to include the restriction that $b \neq 0$ in the definition of the set A?
   (c) Determine an equation that gives a relation between a and b if $(a, b) \in A$ and $(a, b) \approx (2, 3)$.
   (d) Determine at least four different elements in [(2, 3)], the equivalence class of (2, 3).
   (e) Use set builder notion to describe [(2, 3)], the equivalence class of (2, 3).
10. For $(a, b)(c, d) \in \mathbb{R} \times \mathbb{R}$, define $(a, b) \sim (c, d)$ if and only if $a^2 + b^2 = c^2 + d^2$. In Exercise (15) of Section 7.2, we proved that $\sim$ is an equivalence relation on $\mathbb{R} \times \mathbb{R}$.

    (a) Determine the equivalence class of (0, 0).
    (b) Use set builder notation (and do not use the symbol $\sim$) to describe the equivalence class of (2, 3) and then give a geometric description of this equivalence class.
    (c) Give a geometric description of a typical equivalence class for this equivalence relation.
    (d) Let $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \geq 0\}$. Prove that there is a one-to-one correspondence (bijection) between $\mathbb{R}^*$ and the set of all equivalence classes for this equivalence relation.
11. Let A be a nonempty set and let $\sim$ be an equivalence relation on A. Prove each of the following:

    (a) For each $a, b \in A$, $a \nsim b$ if and only if $[a] \cap [b] = \emptyset$.
    (b) For each $a, b \in A$, if $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$.
    (c) For each $a, b \in A$, if $[a] \cap [b] \neq \emptyset$ then $[a] = [b]$.

Explorations and Activities

12. **A Partition Defines an Equivalence Relation**. Let $A = \{a, b, c, d, e\}$ and let $\mathcal{C} = \{\{a, b, c\}, \{d, e\}\}$.

    (a) Explain why $\mathcal{C}$ is a partition of A.

    Define a relation $\sim$ on A as follows: For $x, y \in A$, $x \sim y$ if and only if there exists a set U in $\mathcal{C}$ such that $x \in U$ and $y \in U$.

(b) Prove that $\sim$ is an equivalence relation on the set A, and then determine all the equivalence classes for $\sim$. How does the collection of all equivalence classes compare to $\mathcal{C}$?

What we did for the specific partition in Part (12b) can be done for any partition of a set. So to generalize Part (12b), we let A be a nonempty set and let $\mathcal{C}$ be a partition of A. We then define a relation $\sim$ on A as follows:
For $x, y \in A$, $x \sim y$ if and only if there exists a set U in $\mathcal{C}$ such that $x \in U$ and $y \in U$.

(c) Prove that $\sim$ is an equivalence relation on the set A.
(d) Let $a \in A$ and let $U \in \mathcal{C}$ such that $a \in U$. Prove that $[a] = U$.

13. **Equivalence Relations on a Set of Matrices.** The following exercises require a knowledge of elementary linear algebra. We let $\mathcal{M}_{n,n}(\mathbb{R}$ be the set of all n by n matrices with real number entries.

(a) Define a relation $\sim$ on $\mathcal{M}_{n,n}(\mathbb{R}$ as follows: For all $A, B \in \mathcal{M}_{n,n}(\mathbb{R}$, $A \sim B$ if and only if there exists an invertible matrix P in $\mathcal{M}_{n,n}(\mathbb{R}$ such that $B = PAP^{-1}$. Is $\sim$ an equivalence relation on $\mathcal{M}_{n,n}(\mathbb{R}$? Justify your conclusion.
(b) Define a relation R on $\mathcal{M}_{n,n}(\mathbb{R}$ as follows: For all $A, B \in \mathcal{M}_{n,n}(\mathbb{R}$, $A\ R\ B$ if and only if det(A) = det(B). Is R an equivalence relation on $\mathcal{M}_{n,n}(\mathbb{R}$? Justify your conclusion.
(c) Let $\sim$ be an equivalence relation on $\mathbb{R}$. Define a relation $\approx$ on $\mathcal{M}_{n,n}(\mathbb{R}$ as follow: For all $A, B \in \mathcal{M}_{n,n}(\mathbb{R}$, $A \approx B$ if and only if det(A) $\sim$ det(B). Is $\approx$ an equivalence relation on $\mathcal{M}_{n,n}(\mathbb{R}$? Justify your conclusion.

Answer

Add texts here. Do not delete this text first.

This page titled 7.3: Equivalence Classes is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

7.4: Modular Arithmetic

PREVIEW ACTIVITY7.4.1: Congruence Modulo 6

For this preview activity, we will only use the relation of congruence modulo 6 on the set of integers.

1. Find five different integers a such that $a \equiv 3$ (mod 6) and find five different integers b such that $b \equiv 4$ (mod 6). That is, find five different integers in [3], the congruence class of 3 modulo 6 and five different integers in [4], the congruence class of 4 modulo 6.
2. Calculate $s = a + b$ using several values of a in [3] and several values of b in [4] from Part (1). For each sum s that is calculated, find r so that $0 \le r < 6$ and $s \equiv r$ (mod 6). What do you observe?
3. Calculate $p = a \cdot b$ using several values of a in [3] and several values of b in [4] from Part (1). For each product p that is calculated, find r so that $0 \le r < 6$ and $p \equiv r$ (mod 6). What do you observe?
4. Calculate $q = a^2$ using several values of a in [3] from Part (1). For each product q that is calculated, find r so that $0 \le r < 6$ and $q \equiv r$ (mod 6). What do you observe?

PREVIEW ACTIVITY 7.4.2: The Remainder When Dividing by 9

If a and b are integers with b > 0, then from the Division Algorithm, we know that there exist unique integers q and r such that $a = bq + r$ and $0 \le r < b$.

In this activity, we are interested in the remainder r. Notice that $r = a - bq$. So, given a and b, if we can calculate q, then we can calculate r.

We can use the "int" function on a calculator to calculate q. [The "int" function is the "greatest integer function." If x is a real number, then int(x) is the greatest integer that is less than or equal to x.]

So, in the context of the Division Algorithm, $q = \text{int}(\frac{a}{b})$. Consequently,

$$r = a - b \cdot \text{int}(\frac{a}{b}).$$

If n is a positive integer, we will let $s(n)$ denote the sum of the digits of n. For example, if $n = 731$, then

$$s(731) = 7 + 3 + 1 = 11.$$

For each of the following values of n, calculate

- The remainder when n is divided by 9, and
- The value of $s(n)$ and the remainder when $s(n)$ is divided by 9.

1. $n = 498$
2. $n = 7319$
3. $n = 4672$
4. $n = 9845$
5. $n = 51381$
6. $n = 305877$

What do you observe?

The Integers Modulo n

Let $n \in \mathbb{N}$. Since the relation of congruence modulo n is an equivalence relation on $\mathbb{Z}$, we can discuss its equivalence classes. Recall that in this situation, we refer to the equivalence classes as congruence classes.

Definition: integers modulo n

Let $n \in \mathbb{N}$. The set of congruence classes for the relation of congruence modulo n on $\mathbb{Z}$ is the set of **integers modulo** n, or the set of integers mod n. We will denote this set of congruence classes by $\mathbb{Z}_n$.

Corollary 7.17 tells us that

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup \cdots \cup [n-1].$$

In addition, we know that each integer is congruent to precisely one of the integers 0, 1, 2, ..., $n-1$. This tells us that one way to represent $\mathbb{Z}_n$ is

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots [n-1]\}.$$

Consequently, even though each integer has a congruence class, the set $\mathbb{Z}_n$ has only n distinct congruence classes.

The set of integers $\mathbb{Z}$ is more than a set. We can add and multiply integers. That is, there are the arithmetic operations of addition and multiplication on the set $\mathbb{Z}$, and we know that $\mathbb{Z}$ is closed with respect to these two operations.

One of the basic problems dealt with in modern algebra is to determine if the arithmetic operations on one set “transfer” to a related set. In this case, the related set is $\mathbb{Z}_n$. For example, in the integers modulo 5, $\mathbb{Z}_5$, is it possible to add the congruence classes [4] and [2] as follows?

$$\begin{aligned} [4] \oplus [2] &= [4+2] \\ &= [6] \\ &= [1]. \end{aligned} \tag{7.4.1}$$

We have used the symbol° to denote addition in $\mathbb{Z}_5$ so that we do not confuse it with addition in $\mathbb{Z}$. This looks simple enough, but there is a problem. The congruence classes [4] and [2] are not numbers, they are infinite sets. We have to make sure that we get the same answer no matter what element of [4] we use and no matter what element of [2] we use. For example,

$9 \equiv 4$ (mod 5) and so [9] = [4]. Also,
$7 \equiv 2$ (mod 5) and so [7] = [2].

Do we get the same result if we add [9] and [7] in the way we did when we added [4] and [2]? The following computation confirms that we do:

$$\begin{aligned} [9] \oplus [7] &= [9+7] \\ &= [16] \\ &= [1]. \end{aligned} \tag{7.4.2}$$

This is one of the ideas that was explored in Preview Activity 7.4.1. The main difference is that in this preview activity, we used the relation of congruence, and here we are using congruence classes. All of the examples in Preview Activity 7.4.1 should have illustrated the properties of congruence modulo 6 in the following table. The left side shows the properties in terms of the congruence relation and the right side shows the properties in terms of the congruence classes.

If $a \equiv 3$ (mod 6) and $b \equiv 4$ (mod 6), then • $(a+b) \equiv (3+4)$ (mod 6); • $(a \cdot b) \equiv (3 \cdot 4)$ (mod 6).	If $[a] = [3]$ and $[b] = [4]$ in $\mathbb{Z}_6$, then • $[a+b] = [3+4]$; • $[a \cdot b] = [3 \cdot 4]$.

These are illustrations of general properties that we have already proved in Theorem 3.28. We repeat the statement of the theorem here because it is so important for defining the operations of addition and multiplication in $\mathbb{Z}_n$.

Theorem 3.28

Let n be a natural number and let a, b, c, and d be integers. Then

1. If $a \equiv b$ (mod n) and $c \equiv d$ (mod n), then $(a+c) \equiv (b+d)$ (mod n).
2. If $a \equiv b$ (mod n) and $c \equiv d$ (mod n), then $ac \equiv bd$ (mod n).
3. If $a \equiv b$ (mod n) and $m \in \mathbb{N}$, then $a^m \equiv b^m$ (mod n).

Proof

Add proof here and it will automatically be hidden

Since $x \equiv y$ (mod n) if and only if $[x] = [y]$, we can restate the result of this Theorem 3.28 in terms of congruence classes in $\mathbb{Z}_n$.

Corollary 7.19.

Let n be a natural number and let a, b, c, and d be integers. Then, in $\mathbb{Z}_n$.

1. If $[a] = [b]$ and $[c] = [d]$, then $[a + c] = [b + d]$.
2. If $[a] = [b]$ and $[c] = [d]$, then $[a \cdot c] = [b \cdot d]$.
3. If $[a] = [b]$ and $m \in \mathbb{N}$, then $[a]^m = [b]^m$.

Because of Corollary 7.19, we know that the following formal definition of addition and multiplication of congruence classes in $\mathbb{Z}_n$ is independent of the choice of the elements we choose from each class. We say that these definitions of addition and multiplication are **well defined**.

Definition

Let $n \in \mathbb{N}$. **Addition and multiplication** in $\mathbb{Z}_n$ are defined as follows: For $[a], [c] \in \mathbb{Z}_n$,

$[a] \oplus [c] = [a + c]$ and $[a] \odot [c] = [ac]$.

The term **modular arithmetic** is used to refer to the operations of addition and multiplication of congruence classes in the integers modulo n.

So if $n \in \mathbb{N}$, then we have an addition and multiplication defined on $\mathbb{Z}_n$, the integers modulo n.

Always remember that for each of the equations in the definitions, the operations on the left, $\oplus$ and $\odot$, are the new operations that are being defined. The operations on the right side of the equations ($+$ and $\cdot$) are the known operations of addition and multiplication in $\mathbb{Z}$.

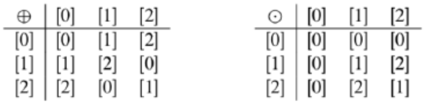
Since $\mathbb{Z}_n$ is a finite set, it is possible to construct addition and multiplication tables for $\mathbb{Z}_n$. In constructing these tables, we follow the convention that all sums and products should be in the form $[r]$, where $0 \le r < n$. For example, in $\mathbb{Z}_3$, we see that by the definition, $[1] \oplus [2] = [3]$, but since $3 \equiv 0$ (mod 3), we see that $[3] = [0]$ and so we write

$$[1] \oplus [2] = [3] = [0]$$

Similarly, by definition, $[2] \odot [2] = [4]$, and in $\mathbb{Z}_3$, [4] = [1]. So we write

$$[2] \odot [2] = [4] = [1]$$

The complete addition and multiplication tables for $\mathbb{Z}_3$ are

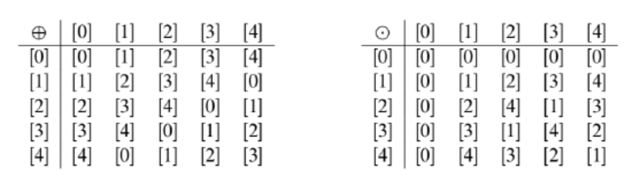


$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\odot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Progress Check 7.20 (Modular Arithmetic in $\mathbb{Z}_2$, $\mathbb{Z}_5$, and $\mathbb{Z}_6$)

1. Construct addition and multiplication tables for $\mathbb{Z}_2$, the integers modulo 2.
2. Verify that the following addition and multiplication tables for $\mathbb{Z}_5$ are correct.



$\oplus$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\odot$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

3. Construct complete addition and multiplication tables for $\mathbb{Z}_6$.
4. In the integers, the following statement is true. We sometimes call this the zero product property for the integers.
   For all $a, b \in \mathbb{Z}$, if $a \cdot b = 0$, then $a = 0$ or $b = 0$.
   Write the contrapositive of the conditional statement in this property.
5. Are the following statements true or false? Justify your conclusions.

   (a) For all $[a], [b] \in \mathbb{Z}_5$, if $[a] \odot [b] = [0]$, then $[a] = [0]$ or $[b] = [0]$.

(b) For all $[a], [b] \in \mathbb{Z}_6$, if $[a] \odot [b] = [0]$, then $[a] = [0]$ or $[b] = [0]$.

Answer

Add texts here. Do not delete this text first.

Divisibility Tests

Congruence arithmetic can be used to proof certain divisibility tests. For example, you may have learned that a natural number is divisible by 9 if the sum of its digits is divisible by 9. As an easy example, note that the sum of the digits of 5823 is equal to $5 + 8 + 2 + 3 = 18$, and we know that 18 is divisible by 9. It can also be verified that 5823 is divisible by 9. (The quotient is 647.) We can actually generalize this property by dealing with remainders when a natural number is divided by 9.

Let $n \in \mathbb{N}$ and let s.n/ denote the sum of the digits of n. For example, if $n = 7319$, then $s(7319) = 7 + 3 + 1 + 9 = 20$. In Preview Activity $7.4.2$, we saw that

$$7319 \equiv 2 \text{ (mod 9) and } 20 \equiv 2 \text{ (mod 9).}$$

In fact, for every example in Preview Activity $7.4.2$, we saw that n and s.n/ were congruent modulo 9 since they both had the same remainder when divided by 9. The concepts of congruence and congruence classes can help prove that this is always true.

We will use the case of $n = 7319$ to illustrate the general process. We must use our standard place value system. By this, we mean that we will write 7319 as follows:

$$7319 = (7 \times 10^3) + (3 \times 10^2) + (1 \times 10^1) + (9 \times 10^0). \tag{7.4.3}$$

The idea is to now use the definition of addition and multiplication in $\mathbb{Z}_9$ to convert equation (7.4.3) to an equation in $\mathbb{Z}_9$. We do this as follows:

$$\begin{aligned} [7319] &= [(7 \times 10^3) + (3 \times 10^2) + (1 \times 10^1) + (9 \times 10^0)] \\ &= [7 \times 10^3] \oplus [3 \times 10^2] \oplus [1 \times 10^1] \oplus [9 \times 10^0] \\ &= ([7] \odot [10^3]) \oplus ([3] \odot [10^2]) \oplus ([1] \odot [10^1]) \oplus ([9] \odot [1]). \end{aligned} \tag{7.4.4}$$

Since $10^3 \equiv 1$ (mod 9), $10^2 \equiv 1$ (mod 9) and $10 \equiv 1$ (mod 9), we can conclude that $[10^3] = [1]$, $[10^2] = [1]$ and $[10] = [1]$. Hence, we can use these facts and equation (7.4.4) to obtain

$$\begin{aligned} [7319] &= ([7] \odot [10^3]) \oplus ([3] \odot [10^2]) \oplus ([1] \odot [10]) \oplus ([9] \odot [1]) \\ &= ([7] \odot [1]) \oplus ([3] \odot [1]) \oplus ([1] \odot [1]) \oplus ([9] \odot [1]) \\ &= [7] \oplus [3] \oplus [1] \oplus [9] \\ &= [7 + 3 + 1 + 9]. \end{aligned} \tag{7.4.5}$$

Equation (7.4.5) tells us that 7319 has the same remainder when divided by 9 as the sum of its digits. It is easy to check that the sum of the digits is 20 and hence has a remainder of 2. This means that when 7319 is divided by 9, the remainder is 2.

To prove that any natural number has the same remainder when divided by 9 as the sum of its digits, it is helpful to introduce notation for the decimal representation of a natural number. The notation we will use is similar to the notation for the number 7319 in equation (7.4.3).

In general, if $n \in \mathbb{N}$, and $n = a_k a_{k-1} \cdots a_1 a_0$ is the decimal representation of n, then

$$n = (a_k \times 10^k) + (a_{k-1} \times 10^{k-1}) + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0).$$

This can also be written using summation notation as follows:

$$n = \sum_{j=0}^{k} (a_j \times 10^j).$$

Using congruence classes for congruence modulo 9, we have

$$\begin{aligned} [n] &= [(a_k \times 10^k) + (a_{k-1} \times 10^{k-1}) + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0)] \\ &= [a_k \times 10^k] \oplus [a_{k-1} \times 10^{k-1}] \oplus \cdots \oplus [a_1 \times 10^1] \oplus [a_0 \times 10^0] \\ &= ([a_k] \odot [10^k]) \oplus ([a_{k-1}] \odot [10^{k-1}]) \oplus \cdots \oplus ([a_1] \odot [10^1]) \oplus ([a_0] \odot [10^0]). \end{aligned} \tag{7.4.6}$$

One last detail is needed. It is given in Proposition 7.21. The proof by mathematical induction is Exercise (6).

Proposition 7.21.

If n is a nonnegative integer, then $10^n \equiv 1$ (mod 9), and hence for the equivalence relation of congruence modulo 9, $[10^n] = [1]$.

If we let $s(n)$ denote the sum of the digits of n, then

$$s(n) = a_k + a_{k-1} + \cdots + a_1 + a_0.$$

Now using equation (7.4.6) and Proposition 7.21, we obtain

\[\begin{array} {rcl} {[n]} &= & {([a_k] \odot [1]) \oplus ([a_{k - 1}] \odot [1]) \oplus \cdot\cdot\cdot \oplus ([a_1] \odot [1]) \oplus ([a_0] \odot [1])} \ {} &= & {[a_k] \oplus [a_{k - 1}] \oplus \cdot\cdot\cdot \oplus [a_1] \oplus [a_0] \ {} &= & {[a_k + a_{k-1} + \cdot\cdot\cdot + a_1 + a_0].} \ {} &= & {[s(n)].} \end{array}\]

This completes the proof of Theorem 7.22.

Theorem 7.22.

Let $n \in \mathbb{N}$ and let $s(n)$ denote the sum of the digits of n. Then

1. $[n] = [s(n)]$, using congruence classes modulo 9.
2. $n \equiv s(n)$ (mod 9)
3. $9 \mid n$ if and only if $9 \mid s(n)$.

Part (3) of Theorem 7.22 is called a **divisibility test**. If gives a necessary and sufficient condition for a natural number to be divisible by 9. Other divisibility tests will be explored in the exercises. Most of these divisibility tests can be proved in a manner similar to the proof of the divisibility test for 9.

Exercise 7.4

1. (a) Complete the addition and multiplication tables for $\mathbb{Z}_4$.
   (b) Complete the addition and multiplication tables for $\mathbb{Z}_7$.
   (c) Complete the addition and multiplication tables for $\mathbb{Z}_8$.
2. The set $\mathbb{Z}_n$ contains n elements. One way to solve an equation in $\mathbb{Z}_n$ is to substitute each of these n elements in the equation to check which ones are solutions. In $\mathbb{Z}_n$, when parentheses are not used, we follow the usual order of operations, which means that multiplications are done first and then additions. Solve each of the following equations:

   (a) $[x]^2 = [1]$ in $\mathbb{Z}_4$
   (b) $[x]^2 = [1]$ in $\mathbb{Z}_8$
   (c) $[x]^4 = [1]$ in $\mathbb{Z}_5$
   (d) $[x]^2 \oplus [3] \odot [x] = [3]$ in $\mathbb{Z}_6$
   (e) $[x]^2 \oplus [1] = [0]$ in $\mathbb{Z}_5$
   (f) $[3] \odot [x] \oplus [2] = [0]$ in $\mathbb{Z}_5$
   (g) $[3] \odot [x] \oplus [2] = [0]$ in $\mathbb{Z}_6$
   (h) $[3] \odot [x] \oplus [2] = [0]$ in $\mathbb{Z}_9$
3. In each case, determine if the statement is true or false.

   (a) For all $[a] \in \mathbb{Z}_6$, if $[a] \neq [0]$, then there exists a $[b] \in \mathbb{Z}_6$ such that $[a] \odot [b] = [1]$.
   (b) For all $[a] \in \mathbb{Z}_5$, if $[a] \neq [0]$, then there exists a $[b] \in \mathbb{Z}_5$ such that $[a] \odot [b] = [1]$.
4. In each case, determine if the statement is true or false.

   (a) For all $[a], [b] \in \mathbb{Z}_6$, if $[a] \neq [0]$ and $[b] \neq [0]$, then $[a] \odot [b] \neq [0]$.
   (b) For all $[a], [b] \in \mathbb{Z}_5$, if $[a] \neq [0]$ and $[b] \neq [0]$, then $[a] \odot [b] \neq [0]$.
5. (a) Prove the following proposition:
   For each $[a] \in \mathbb{Z}_5$, if $[a] \neq [0]$, then $[a]^2 = [1]$ or $[a]^2 = [4]$.
   (b) Does there exist an integer a such that $a^2 = 5,158,232,468,953,153$? Use your work in Part (a) to justify your conclusion. Compare to Exercise (10) in Section 3.5.

6. Use mathematical induction to prove Proposition 7.21.
   If n is a nonnegative integer, then $10^n \equiv 1$ (mod 9), and hence for the equivalence relation of congruence modulo 9, $[10^n] = [1]$.
7. Use mathematical induction to prove that if n is a nonnegative integer, then $10^n \equiv 1$ (mod 3). Hence, for congruence classes modulo 3, if n is a nonnegative integer, then $[10^n] = [1]$.
8. Let $n \in \mathbb{N}$ and let $s(n)$ denote the sum of the digits of n.So if we write

   $$n = (a_k \times 10^k \backslash) {+} (a_{k-1} \times 10^{k-1} + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0). \tag{7.4.7}$$

   then $s(n) = a_k + a_{k-1} + \cdots + a_1 + a_0$. Use the result in Exercise (7) to help prove each of the following:

   (a) $[n] = [s(n)]$, using congruence classes modulo 3.
   (b) $n \equiv s(n)$ (mod 3).
   (c) $3 \mid n$ if only if $3 \mid s(n)$.
9. Use mathematical induction to prove that if n is an integer and $nge1$, then $10^n \equiv 0$ (mod 5). Hence, for congruence classes modulo 5, if n is an integer and $n \geq 1$, then $[10^n] = [0]$.
10. Let $n \in \mathbb{N}$ and assume

    $$n = (a_k \times 10^k) {+} (a_{k-1} \times 10^{k-1} + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0). \tag{7.4.8}$$

    Use the result in Exercise (9) to help prove each of the following:

    (a) $[n] = [a_0]$, using congruence classes modulo 5.
    (b) $n \equiv a_0$ (mod 5).
    (c) $5 \mid n$ if only if $5 \mid a_0$.
11. Use mathematical induction to prove that if n is an integer and $nge2$, then $10^n \equiv 0$ (mod 4). Hence, for congruence classes modulo 4, if n is an integer and $n \geq 2$, then $[10^n] = [0]$.
12. Let $n \in \mathbb{N}$ and assume

    $$n = (a_k \times 10^k) {+} (a_{k-1} \times 10^{k-1} + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0). \tag{7.4.9}$$

    Use the result in Exercise (11) to help prove each of the following:

    (a) $[n] = [10a_1 + a_0]$, using congruence classes modulo 4.
    (b) $n \equiv (10a_1 + a_0)$ (mod 5).
    (c) $4 \mid n$ if only if $4 \mid (10a_1 + a_0)$.
13. Use mathematical induction to prove that if n is an integer and $nge3$, then $10^n \equiv 0$ (mod 8). Hence, for congruence classes modulo 8, if n is an integer and $n \geq 3$, then $[10^n] = [0]$.
14. Let $n \in \mathbb{N}$ and assume

    $$n = (a_k \times 10^k) {+} (a_{k-1} \times 10^{k-1} + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0). \tag{7.4.10}$$

    Use the result in Exercise (13) to help develop a divisibility test for 8. Prove that your divisibility test is correct.
15. Use mathematical induction to prove that if n is a nonnegative integer then $10^n \equiv (-1)^n (mod 11)$. Hence, for congruence classes modulo 11, if n is a nonnegative integer, then $[10^n] = [(-1)^n]$.
16. Let $n \in \mathbb{N}$ and assume

    $$n = (a_k \times 10^k) {+} (a_{k-1} \times 10^{k-1} + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0). \tag{7.4.11}$$

    Use the result in Exercise (15) to help prove each of the following:

    (a) $n \equiv \sum_{j=0}^{k} (-1)^j a_j$ (mod 11).

(b) $[n] = [\sum_{j=0}^{k}(-1)^j a_j]$, using congruence classes modulo 11.
(c) 11 divides n if and only if 11 divides $\sum_{j=0}^{k}(-1)^j a_j$

17. (a) Prove the following proposition:
For all $[a], [b] \in \mathbb{Z}_3$, if $[a]^2 + [b]^2 = [0]$, then $[a] = 0$ and $[b] = [0]$.
(b) Use Exercise (17a) to prove the following proposition:
Let $a, b \in \mathbb{Z}$. If $(a^2 + b^2) \equiv 0 \pmod 3$, then $a \equiv 0 \pmod 3$ and $b \equiv 0 \pmod 3$.
(c) Use Exercise (17b) to prove the following proposition:
Let $a, b \in \mathbb{Z}$, if 3 divides $(a^2 + b^2)$, then 3 divides a and 3 divides b.
18. Prove the following proposition:
For each $a \in \mathbb{Z}$, if there exist integers b and c such that $a = b^4 + c^4$, then the units digit of a must be 0, 1, 2, 5, 6, or 7.
19. Is the following proposition true or false? Justify your conclusion.
For $n \in \mathbb{Z}$. If n is odd, then $8 \mid (n^2 - 1)$. **Hint**: What are the possible values of $n \pmod 8$?
20. Prove the following proposition:
For $n \in \mathbb{Z}$. If $n \equiv 7 \pmod 8$, then n is not the sum of three squares. That is, there do not exist natural numbers a, b, and c such that $n = a^2 + b^2 + c^2$.

Explorations and Activities

21. Using Congruence Modulo 4. The set $\mathbb{Z}_n$ is a finite set, and hence one way to prove things about $\mathbb{Z}_n$ is to simply use the n elements in $\mathbb{Z}_n$ as the n cases for a proof using cases. For example, if $n \in \mathbb{Z}$, then in $\mathbb{Z}_4$, $[n] = [0]$, $[n] = [1]$, $[n] = [2]$, or $[n] = [3]$.

(a) Prove that if $n \in \mathbb{Z}$, then in $\mathbb{Z}_4$, $[n]^2 = [0]$ or $[n]^2 = [1]$. Use this to conclude that in $\mathbb{Z}_4$, $[n^2] = [0]$ or $[n^2] = [1]$.
(b) Translate the equations $[n^2] = [0]$ and $[n^2] = [1]$ in $\mathbb{Z}_4$ into congruences modulo 4.
(c) Use a result in Exercise (12) to determine the value of r so that $r \in \mathbb{Z}$, $0 \le r < 3$, and

$$104\ 257\ 833\ 259 \equiv r \pmod 4). \tag{7.4.12}$$

That is, $[104\ 257\ 833\ 259] = [r]$ in $\mathbb{Z}_4$.
(d) Is the natural number 104 257 833 259 a perfect square? Justify your conclusion.

Answer

Add texts here. Do not delete this text first.

This page titled 7.4: Modular Arithmetic is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

7.S: Equivalence Relations (Summary)

Important Definitions

- Relation from A to B, page 364
- Relation on A, page 364
- Domain of a relation, page 364
- Range of a relation, page 364
- Inverse of a relation, page 373
- Reflexive relation, page 375
- Symmetric relation, page 375
- Transitiverelation,page375
- Equivalence relation, page 378
- Equivalence class, page 391
- Congruence class, page 392
- Partition of a set, page 395
- Integers modulo n, page 402
- Addition in $\mathbb{Z}_n$, page 404
- Multiplication in $\mathbb{Z}_n$, page 404

Important Theorems and Results about Relations, Equivalence Relations, and Equivalence Classes

- **Theorem 7.6.** Let R be a relation from the set A to the set B. Then

  1. The domain of R^{-1} is range of R. That is, dom(R^{-1}) = range(R).
  2. The range of R^{-1} is domain of R. That is, range(R^{-1}) = dom(R).
  3. The inverse of R^{-1} is R. That is, $(R^{-1})^{-1} = R$.
- **Theorem 7.10.** Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. Then $a \equiv b$ (mod n if and only if a and b have the same remainder when divided by n.
- **Theorem 7.14.** Let A be a nonempty set and let $\sim$ be an equivalence relation on A.

  1. For each $a \in A$, $a \in [a]$.
  2. For each $a, b \in A$, $a \sim b$ if and only if $[a] = [b]$.
  3. For each $a, b \in A$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.
- **Corollary 7.16.** Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, let $[a]$ represent the congruence class of a modulo n.

  1. For each $a \in \mathbb{Z}$, $a \in [a]$.
  2. For each $a, b \in \mathbb{Z}$, $a \equiv b$ (mod n) if and only if $[a] = [b]$.
  3. For each $a, b \in \mathbb{Z}$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.
- **Corollary 7.17.** Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, let $[a]$ represent the congruence class of a modulo n.

  1. $\mathbb{Z} = [0] \cup [1] \cup [2] \cup \cdots \cup [n-1]$
  2. For $j, k \in \{0, 1, 2, ..., n-1\}$, if $j \neq k$, then $[j] \cap [k] = \emptyset$.
- Theorem 7.18. Let $\sim$ be an equivalence relation on the nonempty set A. Then the collection $\mathcal{C}$ of all equivalence classes determined by $\sim$ is a partition of the set A.

This page titled 7.S: Equivalence Relations (Summary) is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

CHAPTER OVERVIEW

8: Topics in Number Theory

8.1: The Greatest Common Divisor
8.2: Prime Numbers and Prime Factorizations
8.3: Linear Diophantine Equations
8.S: Topics in Number Theory (Summary)

Thumbnail: Golden spiral. Assuming a square has the side length of 1, the next smaller square is 1/φ wide. Then a width of $1/\varphi^2$, $1/\varphi^3$ and so on. (Public Domain; Jahobr).

This page titled 8: Topics in Number Theory is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

8.1: The Greatest Common Divisor

Preview Activity 8.1.1: The Greatest Common Divisor

1. Explain what it means to say that a nonzero integer m divides an integer n. Recall that we use the notation $m \mid n$ to indicate that the nonzero integer m divides the integer n.
2. Let m and n be integers with $m \neq 0$. Explain what it means to say that m does not divide n.

Definition

Let a and b be integers, not both 0. A **common divisor** of a and b is any nonzero integer that divides both a and b. The largest natural number that divides both a and b is called the **greatest common divisor** of a and b. The greatest common divisor of a and b is denoted by gcd(a, b).

1. Use the roster method to list the elements of the set that contains all the natural numbers that are divisors of 48.
2. Use the roster method to list the elements of the set that contains all the natural numbers that are divisors of 84.
3. Determine the intersection of the two sets in Parts (3) and (4). This set contains all the natural numbers that are common divisors of 48 and 84.
4. What is the greatest common divisor of 48 and 84?
5. Use the method suggested in Parts (3) through (6) to determine each of the following: gcd (8, -12), gcd (0, 5), gcd (8, 27), and gcd (14, 28).
6. If a and b are integers, make a conjecture about how the common divisors of a and b are related to the greatest common divisor of a and b.

Preview Activity 8.1.2: The GCD and the Division Algorithm

When we speak of the quotient and the remainder when we “divide an integer a by the positive integer b,” we will always mean the quotient q and the remainder r guaranteed by the Division Algorithm. (See Section 3.5, page 143.)

1. Each row in the following table contains values for the integers a and b. In this table, the value of r is the remainder (from the Division Algorithm) when a is divided by b. Complete each row in this table by determining gcd(a, b), r, and gcd(b, r).

a	b	gcd(a, b)	Remainder r	gcd(b, r)
44	12			
75	21			
50	33			

2. Formulate a conjecture based on the results of the table in Part (1).

The System of Integers

Number theory is a study of the system of integers, which consists of the set of integers, $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ and the various properties of this set under the usual operations of addition and multiplication and under the usual ordering relation of “less than.” The properties of the integers in Table 8.1 will be considered axioms in this text.

Table 8.1: Axioms for the Integers

	For all integers a, b, and c;
Closure Properties for Addition and Multiplication	$a + b \in \mathbb{Z}$ and $ab \in \mathbb{Z}$
Commutative Properties for Addition and Multiplication	$a + b = b + a$, and $ab = ba$
Associative Properties for Addition and Multiplication	$(a + b) + c = a + (b + c)$ and $(ab)\ c = a\ (bc)$
Distributive Properties of Multiplication over Addition	$a\ (b + c) = (ab + ac)$, and $(b + c)\ a = ba + ca$

	For all integers a, b, and c;
Additive and Multiplicative Identity Properties	$a+0=0+a=a$, and $a\cdot 1=1\cdot a=a$
Additive Inverse Property	\(a + (-a) = (-a) + a = 0

We will also assume the properties of the integers shown in Table 8.2. These properties can be proven from the properties in Table 8.1. (However, we will not do so here.)

Table 8.2: Properties of the Integers

Zero Property of Multiplication	If $a\in\mathbb{Z}$, then $a\cdot 0=0\cdot a=0$.
Cancellation Properties of Addition and Multiplication	If $a,b,c\in\mathbb{Z}$, and $a+b=a+c$, then $b=c$. If $a,b,c\in\mathbb{Z}$, $a\neq 0$ and $ac=bc$, then $b=c$.

We have already studied a good deal of number theory in this text in our discussion of proof methods. In particular, we have studied even and odd integers, divisibility of integers, congruence, and the Division Algorithm. See the summary for Chapter 3 for a summary of results concerning even and odd integers as well as results concerning properties of divisors. We reviewed some of these properties and the Division Algorithm in the Preview Activities.

The Greatest Common Divisor

One of the most important concepts in elementary number theory is that of the greatest common divisor of two integers. The definition for the greatest common divisor of two integers (not both zero) was given in Preview Activity $8.1.1$.

1. If $a,b\in\mathbb{Z}$ and a and b are not both 0, and if $d\in\mathbb{N}$, then $d=\text{gcd}\ (a,b)$ provided that it satisfies all of the following properties:
    - $d\mid a$ and $d\mid b$. That is, d is a common divisor of a and b.
    - If k is a natural number such that $k\mid a$ and $k\mid b$, then $k\leq d$.That is, any other common divisor of a and b is less than or equal to d.
2. Consequently, a natural number d is not the greatest common divisor of a and b provided that it does not satisfy at least one of these properties. That is, d is not equal to gcd(a, b) provided that
    - • d does not divide a or d does not divide b; or
    - • There exists a natural number k such that $k\mid a$ and $k\mid b$ and $k>d$.
3. This means that d is not the greatest common divisor of a and b provided that it is not a common divisor of a and b or that there exists a common divisor of a and b that is greater than d.

In the preview activities, we determined the greatest common divisors for several pairs of integers. The process we used was to list all the divisors of both integers, then list all the common divisors of both integers and, finally, from the list of all common divisors, find the greatest (largest) common divisor. This method works reasonably well for small integers but can get quite cumbersome if the integers are large. Before we develop an efficient method for determining the greatest common divisor of two integers, we need to establish some properties of greatest common divisors.

One property was suggested in Preview Activity $8.1.1$. If we look at the results in Part (7) of that preview activity, we should observe that any common divisor of a and b will divide gcd(a, b). In fact, the primary goals of the remainder of this section are

1. To find an efficient method for determining gcd(a, b), where a and b are integers.
2. To prove that the natural number gcd(a, b) is the only natural number d that satisfies the following properties:

- d divides a and d divides b; and
- if k is a natural number such that $k\mid a$ and $k\mid b$, then $k\mid d$.

The second goal is only slightly different from the definition of the greatest common divisor. The only difference is in the second condition where $k\leq d$ is replaced by $k\mid d$.

We will first consider the case where a and b are integers with $a\neq 0$ and $b>0$. The proof of the result stated in the second goal contains a method (called the Euclidean Algorithm) for determining the greatest common divisors of the two integers a and b. The main idea of the method is to keep replacing the pair of integers .a; b/ with another pair of integers .b; r/, where $0\leq r<b$ and gcd.b;

r/ D gcd.a; b/. This idea was explored in Preview Activity 8.1.2. Lemma 8.1is a conjecture that could have been formulated in Preview Activity 8.1.2.

Lemma 8.1.

Let c and d be integers, not both equal to zero. If q and r are integers such that $c = d \cdot q + r$, then gcd(c, d) = gcd(d, r).

Proof

Let c and d be integers, not both equal to zero. Assume that q and r are integers such that $c = d \cdot q + r$. For ease of notation, we will let

$$m = \text{gcd}(c, d) \text{ and } n = \text{gcd}(d, r).$$

Now, m divides c and m divides d. Consequently, there exist integers x and y such that $c = mx$ and $d = my$. Hence,

$$\begin{aligned} r &= c - d \cdot q \\ r &= mx - (my)q \\ r &= m(x - yq). \end{aligned} \tag{8.1.1}$$

But this means that m divides r. Since m divides d and m divides r, m is less than or equal to gcd(d, r). Thus, $m \le n$.

Using a similar argument, we see that n divides d and n divides r. Since $c = d \cdot q + r$, we can prove that n divides c. Hence, n divides c and n divides d. Thus, $n \le$ gcd(c, d) or $n \le m$. We now have $m \le n$ and $n \le m$. Hence, $m = n$ and gcd(c, d) = gcd(d, r).

Progress Check 8.2: Illustrations of Lemma 8.1

We completed several examples illustrating Lemma 8.1 in Preview Activity 8.1.2. For another example, let $c = 56$ and $d = 12$. The greatest common divisor of 56 and 12 is 4.

1. According to the Division Algorithm, what is the remainder r when 56 is divided by 12?
2. What is the greatest common divisor of 12 and the remainder r?

   The key to finding the greatest common divisor (in more complicated cases) is to use the Division Algorithm again, this time with 12 and r. We now find integers q_2 and r_2 such that

$$12 = r \cdot q_2 + r_2. \tag{8.1.2}$$

3. What is the greatest common divisor of r and r_2?

Answer

Add texts here. Do not delete this text first.

The Euclidean Algorithm

The example in Progress Check 8.2 illustrates the main idea of the **Euclidean Algorithm** for finding gcd(a, b), which is explained in the proof of the following theorem.

Theorem 8.3: Euclidean Algorithm

Let a and b be integers with $a \ne 0$ and $b > 0$. Then gcd(a, b) is the only natural number d such that

(a) d divides a and d divides b, and
(b) if k is an integer that divides both a and b, then k divides d.

Proof

Let a and b be integers with $a \ne 0$ and $b > 0$, and let $d = \text{gcd}(a, b)$. By the Division Algorithm, there exist integers q_1 and r_1 such that

$$a = b \cdot q + r \text{ and } 0 \le r < b \tag{8.1.3}$$

$$a = b \cdot q_1 + r_1, \text{ and } 0 \le r_1 < b. \tag{8.1.3}$$

If $r_1 = 0$, then equation (8.1.3) implies that b divides a. Hence, $b = d = \gcd(a,\, b)$ and this number satisfies Conditions (a) and (b).

If $r_1 > 0$, then by Lemma 8.1, gcd(a, b) = gcd(b, r_1). We use the Division Algorithm again to obtain integers q_2 and r_2 such that

$$b = r_1 \cdot q_2 + r_2, \text{ and } 0 \le r_2 < r_1. \tag{8.1.4}$$

If $r_2 = 0$, then equation (8.1.4) implies that r_1 divides b. This means that $r_1 = \gcd(b,\, r_1)$. But we have already seen that gcd(a, b) = gcd(b, r_1). Hence, $r_1 = \gcd(a,\, b)$. In addition, if k is an integer that divides both a and b, then, using equation (8.1.3), we see that $r_1 = a - b \cdot q_1$ and, hence k divides r_1. This shows that r_1 = gcd(a, b) satisfies Conditions (a) and (b).

If $r_2 > 0$, then by Lemma 8.1, gcd(b, r_1) = gcd(r_1, r_2). But we have already seen that gcd(a, b) = gcd(b, r_1). Hence, gcd(a, b) = gcd(r_1, r_2). We now continue to apply the Division Algorithm to produce a sequence of pairs of integers (all of which have the same greatest common divisor). This is summarized in the following table:

Original Pair	Equation from Division	Inequality from Division Algorithm	New Pair
(a, b)	$a = b \cdot q_1 + r_1$	$0 \le r_1 < b$	(b, r_1)
(b, r_1)	$b = r_1 \cdot q_2 + r_2$	$0 \le r_2 < r_1$	(r_1, r_2)
(r_1, r_2)	$r_1 = r_2 \cdot q_1 + r_3$	$0 \le r_3 < r_2$	(r_2, r_3)
(r_2, r_3)	$r_2 = r_3 \cdot q_1 + r_4$	$0 \le r_4 < r_3$	(r_3, r_4)
(r_3, r_4)	$r_3 = r_4 \cdot q_1 + r_5$	$0 \le r_5 < r_4$	(r_4, r_5)
...	...	...	...

From the inequalities in the third column of this table, we have a strictly decreasing sequence of nonnegative integers ($b > r_1 > r_2 > r_3 > r_4 \cdots$). Consequently, a term in this sequence must eventually be equal to zero. Let p be the smallest natural number such that $r_{p+1} = 0$. This means that the last two rows in the preceding table will be

Original Pair	**Equation from Division Algorithm**	**Inequality from Division Algorithm**	**New Pair**
(r_{p-2}, r_{p-1})	$r_{p-2} = r_{p-1} \cdot q_p + r_p$	$0 \le r_p < r_{p-1}$	(r_{p-1}, r_p)
(r_{p-1}, r_p)	$r_{p-1} = r_p \cdot q_{p+1} + 0$		

Remember that this table was constructed by repeated use of Lemma 8.1 and that the greatest common divisor of each pair of integers produced equals gcd(a, b). Also, the last row in the table indicates that r_p divides r_{p-1}. This means that $\gcd(r_{p-1}, r_p) = r_p$ and hence $r_p = \gcd(a,\, b)$.

This proves that $r_p = \gcd(a,\, b)$ satisfies Condition (a) of this theorem. Now assume that k is an integer such that k divides a and k divides b. We proceed through the table row by row. First, since $r_1 = a - b \cdot q$, we see that

$$k \text{ must divide } r_1.$$

The second row tells us that $r_2 = b - r_1 \cdot q_2$. Since k divides b and k divides r_1, we conclude that

$$k \text{ divides } r_2.$$

Continuing with each row, we see that k divides each of the remainders $r_1, r_2, r_3, ..., r_p$. This means that $r_p = \gcd(a,\, b)$ satisfies Condition (b) of the theorem.

Progress Check 8.4 (Using the Euclidean Algorithm)

1. Use the Euclidean Algorithm to determine gcd(180, 126). Notice that we have deleted the third column (Inequality from Division Algorithm) from the following table. It is not needed in the computations.

Original Pair	Equation from Division Algorithm	New Pair
(180, 126)	$180 = 126 \cdot 1 + 54$	(126, 54)
(126, 54)	126 =	

Consequently, gcd(180, 126) = .

2. Use the Euclidean Algorithm to determine gcd(4208, 288).

Original Pair	Equation from Division Algorithm	New Pair
(4208, 288)	$4208 = 288 \cdot 14 + 176$	(288,)

Consequently, gcd(4208, 288) = .

Answer

Add texts here. Do not delete this text first.

Some Remarks about Theorem 8.3

Theorem 8.3 was proven with the assumptions that $a, b \in \mathbb{Z}$ with $a \neq 0$ and $b > 0$. A more general version of this theorem can be proven with $a, b \in \mathbb{Z}$ and $b = 0$. This can be proven using Theorem 8.3 and the results in the following lemma.

Lemma 8.5.

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then

1. gcd(0, b) = |b|.
2. If gcd(a, b) = d, then gcd(a, $-b$) = d.

The proofs of these results are in Exercise (4). An application of this result is given in the next example.

Example 8.6 (Using the Euclidean Algorithm)

Let $a = 234$ and $b = -42$. We will use the Euclidean Algorithm to determine gcd(234, 42).

Step	Original Pair	Equation from Division Algorithm	New Pair
1	(234, 42)	$234 = 42 \cdot 5 + 24$	(42, 24)
2	(42, 24)	$42 = 24 \cdot 1 + 18$	(24, 18)
3	(24, 18)	$24 = 18 \cdot 1 + 6$	(18, 6)
4	(18, 6)	$18 = 6 \cdot 3$	

So gcd(234, 42) = 6 and hence gcd(234, -42) = 6.

Writing gcd(a, b) in Terms of a and b

We will use Example 8.6 to illustrate another use of the Euclidean Algorithm. It is possible to use the steps of the Euclidean Algorithm in reverse order to write gcd(a, b) in terms of a and b. We will use these steps in reverse order to find integers m and n such that gcd(234, 42) = 234m + 42n. The idea is to start with the row with the last nonzero remainder and work backward as shown in the following table:

Explanation	Result
First, use the equation in Step 3 to write 6 in terms of 24 and 18.	$6 = 24 - 18 \cdot 1$
Use the equation in Step 2 to write \(18 = 42 - 24 \cdot 1\). Substitute this into the preceding result and simplify.	$\begin{aligned} 6 &= 24 - 18 \cdot 1 \\ &= 24 - (42 - 24 \cdot 1) \\ &= 42 \cdot (-1) + 24 \cdot 2 \end{aligned}$
We now have written 6 in terms of 42 and 24. Use the equation in Step 1 to write $24 = 234 - 42 \cdot 5$. Substitute this into the preceding result and simplify.	$\begin{aligned} 6 &= 42 \cdot (-1) + 24 \cdot 2 \\ &= 42 \cdot (-1) + (234 - 42 \cdot 5) \cdot 2 \\ &= 234 \cdot 2 + 42 \cdot (-11) \end{aligned}$

Hence, we can write

$$\gcd(234, 42) = 234 \cdot 2 + 42 \cdot (-11).$$

(Check this with a calculator.) In this case, we say that we have written gcd(234, 42) as a linear combination of 234 and 42. More generally, we have the following definition.

Definition

Let a and b be integers. A linear combination of a and b is an integer of the form $ax + by$, where x and y are integers.

Progress Check 8.7 (Writing the gcd as a Linear Combination)

Use the results from Progress Check 8.4 to

1. Write gcd(180, 126) as a linear combination of 180 and 126.
2. Write gcd(4208, 288) as a linear combination of 4208 and 288.

Answer

Add texts here. Do not delete this text first.

The previous example and progress check illustrate the following important result in number theory, which will be used in the next section to help prove some other significant results.

Theorem 8.8

Let a and b be integers, not both 0. Then gcd(a, b) can be written as a linear combination of a and b. That is, there exist integers u and v such that $\gcd(a, b) = au + bv$.

We will not give a formal proof of this theorem. Hopefully, the examples and activities provide evidence for its validity. The idea is to use the steps of the Euclidean Algorithm in reverse order to write gcd(a, b) as a linear combination of a and b. For example, assume the completed table for the Euclidean Algorithm is

Step	Original Pair	Equation from Division Algorithm	New Pair
1	(a, b)	$a = b \cdot q_1 + r_1$	(b, r_1)
2	(b, r_1)	$b = r_1 \cdot q_2 + r_2$	(r_1, r_2)
3	(r_1, r_2)	$r_1 = r_2 \cdot q_3 + r_3$	(r_2, r_3)

4	(r_2, r_3)	$r_2 = r_3 \cdot q_4 + 0$	(r_3, r_4)

We can use Step 3 to write $r_3 = \gcd(a, b)$ as a linear combination of r_1 and r_2. We can then solve the equation in Step 2 for r_2 and use this to write $r_3 = \gcd(a, b)$ as a linear combination of r_1 and b. We can then use the equation in Step 1 to solve for r_1 and use this to write $r_3 = \gcd(a, b)$ as a linear combination of a and b.

In general, if we can write $r_p = \gcd(a, b)$ as a linear combination of a pair in a given row, then we can use the equation in the preceding step to write $r_p = \gcd(a, b)$ as a linear combination of the pair in this preceding row.

The notational details of this induction argument get quite involved. Many mathematicians prefer to prove Theorem 8.8 using a property of the natural numbers called the Well-Ordering Principle. **The Well-Ordering Principle** for the natural numbers states that any nonempty set of natural numbers must contain a least element. It can be proven that the Well-Ordering Principle is equivalent to the Principle of Mathematical Induction.

? Exercise 8.1

1. Find each of the following greatest common divisors by listing all of the common divisors of each pair of integers.

   (a) gcd(21, 28)
   (b) gcd(-21, 28)
   (c) gcd(58, 63)
   (d) gcd(0, 12)
   (e) gcd(110, 215)
   (f) gcd(110, -215)
2. (a) Let $a \in \mathbb{Z}$ and let $k \in \mathbb{Z}$ with $k \neq 0$. Prove that if $k \mid a$ and $k \mid (a+1)$, then $k \mid 1$, and hence $k = \pm 1$.
   (b) Let $a \in \mathbb{Z}$. Find the greatest common divisor of the consecutive integers a and $a+1$. That is, determine gcd(a, $a+1$).
3. (a) Let $a \in \mathbb{Z}$ and let $k \in \mathbb{Z}$ with $k \neq 0$. Prove that if $k \mid a$ and $k \mid (a+2)$, then $k \mid 2$.
   (b) Let $a \in \mathbb{Z}$. Find the greatest common divisor of the common divisor a and $a+2$.
4. Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Prove each of the following:

   (a) gcd(0, b) = $|b|$
   (b) If gcd(a, b) = d, then gcd(a, $-b$) = d. That is, gcd(a, $-b$) = gcd(a, b).
5. For each of the following pairs of integers, use the Euclidean Algorithm to find gcd(a, b) and to write gcd(a, b) as a linear combination of a and b. That is, find integers m and n such that $d = am + bn$.

   (a) $a = 36$, $b = 60$
   (b) $a = 901$, $b = 935$
   (c) $a = 72$, $b = 714$
   (d) $a = 12528$, $b = 21361$
   (e) $a = -36$, $b = -60$
   (f) $a = 901$, $b = -935$
6. (a) Find integers u and v such that $9u + 14v = 1$ or explain why it is not possible to do so. Then find integers x and y such that $9x + 14y = 10$ or explain why it is not possible to do so.
   (b) Find integers x and y such that $9x + 15y = 10$ or explain why it is not possible to do so.
   (c) Find integers x and y such that $9x + 15y = 3162$ or explain why it is not possible to do so.
7. (a) Notice that gcd(11, 17) = 1. Find integers x and y such that $11x + 17y = 1$.
   (b) Let $m, n \in \mathbb{Z}$. Wrtie the sum $\frac{m}{11} + \frac{n}{17}$ as a single fraction.
   (c) Find two rational numbers with denominators of 11 and 17, respectively, whose sum is equal to $\frac{10}{187}$. **Hint**: Write the rational numbers in the form $\frac{m}{11} + \frac{n}{17}$, where $m, n \in \mathbb{Z}$. Then write

$$\frac{m}{11} + \frac{n}{17} = \frac{10}{187}. \tag{8.1.5}$$

Use Exercises (7a) and (7b) to determine m and n.

(d) Find two rational numbers with denominators 17 and 21, respectively, whose sum is equal to $\frac{326}{357}$ or explain why it is not possible to do so.

(e) Find two rational numbers with denominators 9 and 15, respectively, whose sum is equal to $\frac{10}{225}$ or explain why it is not possible to do so.

Exploration and Activities

8. **Linear Combinations and the Greatest Common Divisor**

(a) Determine the greatest common divisor of 20 and 12?
(b) Let $d = \gcd(20, 12)$. Write d as a linear combination of 20 and 12.
(c) Generate at least six different linear combinations of 20 and 12. Are these linear combinations of 20 and 12 multiples of gcd(20, 12)?
(d) Determine the greatest common divisor of 21 and -6 and then generate at least six different linear combinations of 21 and -6. Are these linear combinations of 21 and -6 multiples of gcd(21, -6)?
(e) The following proposition was first introduced in Exercise (18) on page 243 in Section 5.2. Complete the proof of this proposition if you have not already done so.

Proposition 5.16

Let a, b, and t be integers with $t \neq 0$. If t divides a and t divides b, then for all integers x and y, t divides $ax + by$

Proof: Let a, b and t be integers with $t \neq 0$, and assume that t divides a and t divides b. We will prove that for all integers x and y, t divides $(ax + by)$.
So let $x \in \mathbb{Z}$ and let $y \in \mathbb{Z}$. Since t divides a, there exists an integer msuch that ...
(f) Now let a and b be integers, not both zero and let $d = \gcd(a, b)$. Theorem 8.8 states that d is a linear combination of a and b. In addition, let S and T be the following sets:

$$S = \{ax + by \mid x, y \in \mathbb{Z}\} \quad \text{and} \quad T = \{kd \mid k \in \mathbb{Z}\}. \tag{8.1.6}$$

That is, S is the set of all linear combinations of a and b, and T is the set of all multiples of the greatest common divisor of a and b. Does the set S equal the set T? If not, is one of these sets a subset of the other set? Justify your conclusions.

Note: In Parts (c) and (d), we were exploring special cases for these two sets.

Answer

Add texts here. Do not delete this text first.

This page titled 8.1: The Greatest Common Divisor is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

8.2: Prime Numbers and Prime Factorizations

? Preview Activity 8.2.1: Exploring Examples where a Divides $b \cdot c$

1. Find at least three different examples of nonzero integers a, b, and c such that $a \mid (bc)$ but a does not divide b and a does not divide c. In each case, compute gcd(a, b) and gcd(a, c).
2. Find at least three different examples of nonzero integers a, b, and c such that gcd(a, b) = 1 and $a \mid (bc)$. In each example, is there any relation between the integers a and c?
3. Formulate a conjecture based on your work in Parts (1) and (2).

? Preview Activity 8.2.2: Prime Factorizations

Recall that a natural number p is a **prime number** provided that it is greater than 1 and the only natural numbers that divide p are 1 and p. A natural number other than 1 that is not a prime number is a **composite number**. The number 1 is neither prime nor composite. (See Exercise 13 from Section 2.4 on page 78.)

1. Give examples of four natural numbers that are prime and four natural numbers that are composite.

Theorem 4.9 in Section 4.2 states that every natural number greater than 1 is either a prime number or a product of prime numbers. When a composite number is written as a product of prime numbers, we say that we have obtained a **prime factorization** of that composite number. For example, since $60 = 2^2 \cdot 3 \cdot 5$, we say that $2^2 \cdot 3 \cdot 5$ is a prime factorization of 60.

2. Write the number 40 as a product of prime numbers by first writing $40 = 2 \cdot 20$ and then factoring 20 into a product of primes. Next, write the number 40 as a product of prime numbers by first writing $40 = 5 \cdot 8$ and then factoring 8 into a product of primes.
3. In Part (2), we used two different methods to obtain a prime factorization of 40. Did these methods produce the same prime factorization or different prime factorizations? Explain.
4. Repeat Parts (2) and (3) with 150. First, start with $150 = 3 \cdot 50$, and then start with $150 = 5 \cdot 30$.

Greatest Common Divisors and Linear Combinations

In Section 8.1, we introduced the concept of the greatest common divisor of two integers. We showed how the Euclidean Algorithm can be used to find the greatest common divisor of two integers, a and b, and also showed how to use the results of the Euclidean Algorithm to write the greatest common divisor of a and b as a linear combination of a and b.

In this section, we will use these results to help prove the so-called Fundamental Theorem of Arithmetic, which states that any natural number greater than 1 that is not prime can be written as product of primes in "essentially" only one way. This means that given two prime factorizations, the prime factors are exactly the same, and the only difference may be in the order in which the prime factors are written. We start with more results concerning greatest common divisors. We first prove Proposition 5.16, which was part of Exercise (18) in Section 5.2 and Exercise (8) in Section 8.1.

Theorem 5.16

Let a, b, and t be integers with $t \neq 0$. If t divides a and t divides b, then for all integers x and y, t divides $(ax + by)$.

Proof

Let a, b, and t be integers with $t \neq 0$, and assuem that t divides a and t divides b. We will prove that for all integers x and y, t divides $(ax + by)$.

So let $x \in \mathbb{Z}$ and let $y \in \mathbb{Z}$. Since t divides a, there exists an integer m such that $a = mt$ and since t divides b, there exists an integer n such that $b = nt$. Using substitution and algebra, we then see that

$$\begin{aligned} ax + by &= (mt)x + (nt)y \\ &= t(mx + ny) \end{aligned} \tag{8.2.1}$$

Since $(mx + ny)$ is an integer, the last equation proves that t divides $ax + by$ and this proves that for all integers x and y, t divides $(ax + by)$.

We now let $a, b \in \mathbb{Z}$, not both 0, and let $d = \gcd(a, b)$. Theorem 8.8 states that d can be written as a linear combination of a and b. Now, since $d \mid a$ and $d \mid b$, we can use the result of Proposition 5.16 to conclude that for all $x, y \in \mathbb{Z}$, $d \mid (ax + by)$. This means that d divides every linear combination of a and b. In addition, this means that d must be the smallest positive number that is a linear combination of a and b. We summarize these results in Theorem 8.9.

Theorem 8.9.

Let $a, b \in \mathbb{Z}$, not both 0.

1. The greatest common divisor, d, is a linear combination of a and b. That is, there exist integers m and n such that $d = am + bn$.
2. The greatest common divisor, d, divides every linear combination of a and b. That is, for all $x, y \in \mathbb{Z}$, $d \mid (ax + by)$.
3. The greatest common divisor, d, is the smallest positive number that is a linear combination of a and b.

Relatively Prime Integers

In Preview Activity $8.2.1$, we constructed several examples of integers a, b, and c such that $a \mid (bc)$ but a does not divide b and a does not divide c. For each example, we observed that $\gcd(a, b) \neq 1$ and $\gcd(a, c) \neq 1$.

We also constructed several examples where $a \mid (bc)$ and $\gcd(a, b) = 1$. In all of these cases, we noted that a divides c. Integers whose greatest common divisor is equal to 1 are given a special name.

Definition: relatively prime

Two nonzero integers a and b are *relatively prime* provided that $\gcd(a, b) = 1$.

Progress Check 8.10: Relatively Prime Integers

1. Construct at least three different examples where p is a prime number, $a \in \mathbb{Z}$, and $p \mid a$. In each example, what is gcd(a, p)? Based on these examples, formulate a conjecture about gcd(a, p) when $p \mid a$.
2. Construct at least three different examples where p is a prime number, $a \in \mathbb{Z}$, and p does not divide a. In each example, what is gcd(a, p)? Based on these examples, formulate a conjecture about gcd(a, p) when p does not divide a.
3. Give at least three different examples of integers a and b where a is not prime, b is not prime, and $\gcd(a, b) = 1$, or explain why it is not possible to construct such examples.

Answer

Add texts here. Do not delete this text first.

Theorem 8.11.

Let a and b be nonzero integers, and let p be a prime number.

1. If a and b are relatively prime, then there exist integers m and n such that $am + bn = 1$. That is, 1 can be written as linear combination of a of b.
2. If $p \mid a$, then $\gcd(a, p) = p$.
3. If p does not divide a, then $\gcd(a, p) = 1$.

Part (1) of Theorem 8.11 is actually a corollary of Theorem 8.9. Parts (2) and (3) could have been the conjectures you formulated in Progress Check 8.10. The proofs are included in Exercise (1).

Given nonzero integers a and b, we have seen that it is possible to use the Euclidean Algorithm to write their greatest common divisor as a linear combination of a and b. We have also seen that this can sometimes be a tedious, time-consuming process, which is why people have programmed computers to do this. Fortunately, in many proofs of number theory results, we do not actually have to construct this linear combination since simply knowing that it exists can be useful in proving results. This will be illustrated in the proof of Theorem 8.12, which is based on work in Preview Activity $8.2.1$.

Theorem 8.12

Let a, b, be nonzero integers and let c be an integer. If a and b are relatively prime and $a \mid (bc)$, then $a \mid c$

The explorations in Preview Activity $8.2.1$ were related to this theorem. We will first explore the forward-backward process for the proof. The goal is to prove that $a \mid c$. A standard way to do this is to prove that there exists an integer q such that

$$c = aq. \tag{8.2.2}$$

Since we are given $a \mid (bc)$, there exists an integer k such that

$$bc = ak. \tag{8.2.3}$$

It may seem tempting to divide both sides of Equation ??? by b, but if we do so, we run into problems with the fact that the integers are not closed under division. Instead, we look at the other part of the hypothesis, which is that a and b are relatively prime. This means that $\gcd(a, b) = 1$. How can we use this? This means that a and b have no common factors except for 1. In light of Equation ???, it seems reasonable that any factor of a must also be a factor of c. But how do we formalize this?

One conclusion that we can use is that since $\gcd(a, b) = 1$, by Theorem 8.11, there exist integers m and n such that

$$am + bn = 1. \tag{8.2.4}$$

We may consider solving equation (8.2.4) for b and substituting this into Equation ???. The problem, again, is that in order to solve Equation ??? for b, we need to divide by n.

Before doing anything else, we should look at the goal in Equation ???. We need to introduce c into Equation ???. One way to do this is to multiply both sides of equation (8.2.4) by c. (This keeps us in the system of integers since the integers are closed under multiplication.) This gives

$$\begin{aligned} (am + bn)c &= 1 \cdot c \\ acm + bcn &= c. \end{aligned} \tag{8.2.5}$$

Notice that the left side of Equation ??? contains a term, bcn, that contains bc. This means that we can use Equation ??? and substitute bc D ak in Equation ???. After doing this, we can factor the left side of the equation to prove that $a \mid c$.

Progress Check 8.13: Completing the Proof of Theorem 8.12

Write a complete proof of Theorem 8.12.

Answer

Add texts here. Do not delete this text first.

Corollary 8.14

1. Let $a, b \in \mathbb{Z}$, and let p be a prime number. If $p \mid (ab)$, then $p \mid a$ or $p \mid b$.
2. Let p be a prime number, let $n \in \mathbb{N}$, and let $a_1, a_2, ..., a_n \in \mathbb{Z}$. If $p \mid (a_1 a_2 \cdots a_n)$, then there exists a natural number k with $1 \le k \le n$ such that $p \mid a_k$.

Part (1) of Corollary 8.14 is a corollary of Theorem 8.12. Part (2) is proved using mathematical induction. The basis step is the case where $n = 1$, and Part (1) is the case where $n = 2$. The proofs of these two results are included in Exercises (2) and (3).

Historical Note: Euclid’s Lemma

Part (1) of Corollary 8.14 is known as *Euclid’s Lemma*. Most people associate geometry with *Euclid’s Elements*, but these books also contain many basic results in number theory. Many of the results that are contained in this section appeared in *Euclid’s Elements*.

Prime Numbers and Prime Factorizations

We are now ready to prove the Fundamental Theorem of Arithmetic. The first part of this theorem was proved in Theorem 4.9 in Section 4.2. This theorem states that each natural number greater than 1 is either a prime number or is a product of prime numbers. Before we state the Fundamental Theorem of Arithmetic, we will discuss some notational conventions that will help us with the proof. We start with an example.

We will use $n = 120$. Since $5 \mid 120$, we can write $120 = 5 \cdot 24$. In addition, we can factor 24 as $24 = 2 \cdot 2 \cdot 2 \cdot 3$. So we can write

$$\begin{aligned} 120 &= 5 \cdot 24 \\ &= 5(2 \cdot 2 \cdot 2 \cdot 3). \end{aligned} \tag{8.2.6}$$

This is a prime factorization of 120, but it is not the way we usually write this factorization. Most often, we will write the prime number factors in ascending order. So we write

$$120 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \text{ or } 120 = 2^3 \cdot 3 \cdot 5.$$

Now, let $n \in \mathbb{N}$. To write the prime factorization of n with the prime factors in ascending order requires that if we write $n = p_1 p_2 \cdots p_r$, where $p_1 p_2 \cdots p_r$ are prime numbers, we will have $p_1 \le p_2 \le \cdots \le p_r$.

Theorem 8.15: The Fundamental Theorem of Arithmetic

1. Each natural number greater than 1 is either a prime number or is a product of prime numbers.
2. let $n \in \mathbb{N}$ with $n > 1$. Assume that

$$n = p_1 p_2 \cdots p_r \text{ and that } n = q_1 q_2 \cdots q_s, \tag{8.2.7}$$

where $p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_s$ are prime with $p_1 \le p_2 \le \cdots \le p_r$ and $q_1 \le q_2 \le \cdots \le q_s$. Then $r = s$, and for each j from 1 to r, $p_j = qj$.

Proof

The first part of this theorem was proved in Theorem 4.9. We will prove the second part of the theorem by induction on n using the Second Principle of Mathematical Induction. (See Section 4.2.) For each natural number n with $n > 1$, let $P(n)$ be

If $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$, where $p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_s$ are primes with $p_1 \le p_2 \le \cdots \le p_r$ and $q_1 \le q_2 \le \cdots \le q_s$, then $r = s$, and for each j from 1 to r, $p_j = qj$.

For the basis step, we notice that since 2 is a prime number, its only factorization is $2 = 1 \cdot 2$. This means that the only equation of the form $n = p_1 p_2 \cdots p_r$, where $p_1 p_2 \cdots p_r$ are prime numbers, is the case where $r = 1$ and $p_1 = 2$.This proves that $P(2)$ is true.

For the inductive step, let $k \in \mathbb{N}$ with $k \ge 2$. We will assume that $P(2), P(3), \ldots, P(k)$ are true. The goal now is to prove that $P(k+1)$ is true. To prove this, we assume that $(k+1)$ has two prime factorizations and then prove that these prime factorizations are the same. So we assume that

$k + 1 = p_1 p_2 \cdots p_r$ and that $k + 1 = q_1 q_2 \cdots q_s$, wher $p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_s$ are prime with $p_1 \le p_2 \le \cdots \le p_r$ and $q_1 \le q_2 \le \cdots \le q_s$.

We must now prove that $r = s$, and for each j from 1 to r, $p_j = q_j$. We can break our proof into two cases: (1) $p_1 \le q_1$; and (2) $q_1 \le p_1$. Since one of these must be true, and since the proofs will be similar, we can assume, without loss of generality, that $p_1 \le q_1$.

Since $k + 1 = p_1 p_2 \cdots p_r$, we know that $p_1 \mid (k+1)$, and hence we may conclude that $p_1 \mid (q_1 q_2 \cdots q_s)$. We now use Corollary 8.14 to conclude that there exists a j with $1 \le j \le s$ such that $p_1 \mid q_j$. Since p_1 and q_j are primes, we conclude that

$$p_1 = q_j.$$

We now use this and the fact that $k + 1 = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ to conclude that

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

The product in the previous equation is less that $k+1$. Hence, we can apply our induction hypothesis to these factorizations and conclude that $r = s$, and for each j from 2 to r, $p_j = q_j$.

This completes the proof that if $P(2), P(3), \ldots, P(k)$ are true, then $P(k+1)$ is true. Hence, by the Second Principle of Mathematical Induction, we conclude that $P(n)$ is true for all $n \in \mathbb{N}$ with $n \geq 2$. This completes the proof of the theorem.

Note: We often shorten the result of the Fundamental Theorem of Arithmetic by simply saying that each natural number greater than one that is not a prime has a **unique factorization** as a product of primes. This simply means that if $n \in \mathbb{N}$, $n > 1$, and n is not prime, then no matter how we choose to factor n into a product of primes, we will always have the same prime factors. The only difference may be in the order in which we write the prime factors.

Further Results and Conjectures about Prime Numbers

1. **The Number of Prime Numbers**
   Prime numbers have fascinated mathematicians for centuries. For example, we can easily start writing a list of prime numbers in ascending order. Following is a list of the prime numbers less than 100.

   2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

   This list contains the first 25 prime numbers. Does this list ever stop? The question was answered in Euclid's Elements, and the result is stated in Theorem 8.16. The proof of this theorem is considered to be one of the classical proofs by contradiction.

Theorem 8.16.

There are infinitely many prime numbers.

Proof

We will use a proof by contradiction. We assume that there are only finitely many primes, and let

$$p_1, p_2, \ldots, p_m$$

be the list of all the primes. Let

$$M = p_1 p_2, \ldots, p_m + 1. \tag{8.2.8}$$

Notice that $M \neq 1$. So M is either a prime number or, by the Fundamental Theorem of Arithmetic, M is a product of prime numbers. In either case, M has a factor that is a prime number. Since we have listed all the prime numbers, this means that there exists a natural number j with $1 \leq j \leq m$ such that $p_j \mid M$. Now, we can rewrite equation (8.2.8) as follows:

$$1 = M - p_1 p_2 \cdots p_m. \tag{8.2.9}$$

We have proved $p_j \mid M$, and since p_j is one of the prime factors of $p_1 p_2 \cdots p_m$, we can also conclude that $p_j \mid (p_1 p_2 \cdots p_m)$. Since p_j divides both of the terms on the right side of equation (8.2.9), we can use this equation to conclude that p_j divides 1. This is a contradiction since a prime number is greater than 1 and cannot divide 1. Hence, our assumption that there are only finitely many primes is false, and so there must be infinitely many primes.

2. There are infinitely many primes, but when we write a list of the prime numbers, we can see some long sequences of consecutive natural numbers that contain no prime numbers. For example, there are no prime numbers between 113 and 127. The following theorem shows that there exist arbitrarily long sequences of consecutive natural numbers containing no prime numbers. A guided proof of this theorem is included in Exercise (15).

Theorem 8.17,

For any natural number n, there exist at least n consecutive natural numbers that are composite numbers.

There are many unanswered questions about prime numbers, two of which will now be discussed.

3. By looking at the list of the first 25 prime numbers, we see several cases where consecutive prime numbers differ by 2. Examples are: 3 and 5; 11 and 13; 17 and 19; 29 and 31. Such pairs of prime numbers are said to be **twin primes**. How many twin primes exist? The answer is not known. The **Twin Prime Conjecture** states that there are infinitely many twin primes. As of June 25, 2010, this is still a conjecture as it has not been proved or disproved.

   For some interesting information on prime numbers, visit the Web site *The Prime Pages* (primes.utm.edu/), where there is a link to The Largest Known Primes Web site. According to information at this site as of June 25, 2010, the largest known twin primes are

$$(65516468355 \times 2^{333333} - 1) \text{ and } (65516468355 \times 2^{333333} + 1). \tag{8.2.10}$$

   Each of these prime numbers contains 100355 digits.

4. Given an even natural number, is it possible to write it as a sum of two prime numbers? For example,

   4 = 2 + 2 6 = 3 + 3 8 = 5 + 3
   78 = 37 + 41 90 = 43 + 47 128 = 67 + 71

   One of the most famous unsolved problems in mathematics is a conjecture made by Christian Goldbach in a letter to Leonhard Euler in 1742. The conjecture, now known as **Goldbach's Conjecture**, is as follows:

   Every even integer greater than 2 can be expressed as the sum of two (not necessarily distinct) prime numbers.

   As of June 25, 2010, it is not known if this conjecture is true or false, al- though most mathematicians believe it to be true.

Exercise 8.2

1. Prove the second and third parts of Theorem 8.11.

   (a) Let a be a nonzero integer, and let p be a prime number. If $p \mid a$, then $\gcd(a, p) = p$.
   (b) Let a be a nonzero integer, and let p be a prime number. If p does not divide a, then $\gcd(a, p) = 1$.
2. Prove the first part of Corollary 8.14.
   Let $a, b \in \mathbb{Z}$, let p be a prime number. If $p \mid (ab)$, then $p \mid a$ or $p \mid b$. **Hint**: Consider two cases: (1) $p \mid a$; and (2) p does not divide a.
3. Use mathematical induction to prove the second part of Corollary 8.14.
   Let p be a prime number, let $n \in \mathbb{N}$, and let $a_1, a_2, ..., a_n \in \mathbb{Z}$. If $p \mid (a_1 a_2 \cdots a_n)$, then there exists a $k \in \mathbb{N}$ with $1 \le k \le n$ such that $p \mid a_k$.
4. (a) Let a and b be nonzero integers. If there exist integers x and y such that $ax + by = 1$, what conclusion can be made about gcd(a, b)? Explain.
   (b) Let a and b be nonzero integers. If there exist integers x and y such that $ax + by = 2$, what conclusion can be made about gcd(a, b)? Explain.
5. (a) Let $a \in \mathbb{Z}$. What is gcd.a; a C 1/? That is, what is the greatest common divisor of two consecutive integers? Justify your conclusion.

   Hint: Exercise (4) might be helpful.

   (b) Let $a \in \mathbb{Z}$. What conclusion can be made about gcd(a, $a + 2$)? That is, what conclusion can be made about the greatest common divisor of two integers that differ by 2? Justify your conclusion.

6. (a) Let $a \in \mathbb{Z}$. What conclusion can be made about gcd(a, $a + 3$)? That is, what conclusion can be made about the greatest common divisor of two integers that differ by 3? Justify your conclusion.
   (b) Let $a \in \mathbb{Z}$. What conclusion can be made about gcd(a, $a + 4$)? That is, what conclusion can be made about the greatest common divisor of two integers that differ by 4? Justify your conclusion.

7. (a) Let $a = 16$ and $b = 28$. Determine the value of $d = \gcd(a, b)$, and then determine the value of gcd($\frac{a}{d}$, $\frac{b}{d}$).

   (b) Repeat Exercise (7a) with $a = 10$ and $b = 45$.

   (c) Let $a, b \in \mathbb{Z}$, not both equal to 0, and let $d = \gcd(a, b)$. Explain why $\frac{a}{d}$ and $\frac{b}{d}$ are integers. Then prove that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

   Hint: Start by writing d as a linear combination of a and b.

   This says that if you divide both a and b by their greatest common divisor, the result will be two relatively prime integers.
8. Are the following propositions true or false? Justify your conclusions.

   (a) For all integers a, b, and c, if $a \mid c$ and $b \mid c$, then $(ab) \mid c$.

   (b) For all integers a, b, and c, if $a \mid c$, $b \mid c$, and $\gcd(a, b) = 1$, then $(ab) \mid c$.
9. In Exercise (16) in Section 3.5, it was proved that if n is an odd integer, then $8 \mid (n^2 - 1$\). (This result was also proved in Exercise (19) in Section 7.4.) Now, prove the following proposition:

   If n is an odd integer and 3 does not divide n, then $24 \mid (n^2 - 1)$.
10. (a) Prove the following proposition:

    For all $a, b, c \in \mathbb{Z}$, $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

    (b) Use mathematical induction to prove the following proposition:

    Let $n \in \mathbb{N}$ and let $a, b_1, b_2, ..., b_n \in \mathbb{Z}$. If $\gcd(a, b_i) = 1$ for all $i \in \mathbb{N}$ with $1 \le i \le n$, then $\gcd(a, b_1 b_2 \cdots b_n) = 1$.
11. Is the following proposition true or false? Justify your conclusion.

    Fro all integer a, b, and c, if $\gcd(a, b) = 1$ and $c \mid (a + b)$, then $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$.
12. Is the following proposition true or false? Justify your conclusion.

    If $n \in \mathbb{N}$, then $\gcd(5n + 2, 12n + 5) = 1$
13. Let $y \in \mathbb{N}$. Use the Fundamental Theorem of Arithmetic to prove that there exists an odd natural number x and a nonnegative integer k such that $y = 2^k x$.
14. (a) Determine five different primes that are congruent to 3 modulo 4.

    (b) Prove that there are infinitely many primes that are congruent to 3 modulo 4.
15. (a) Let $n \in \mathbb{N}$. Prove that 2 divides $[(n + 1)! + 2]$.

    (b) Let $n \in \mathbb{N}$ with $n \ge 2$. Prove that 3 divides $[(n + 1)! + 3]$.

    (c) Let $n \in \mathbb{N}$. Prove that for each $k \in \mathbb{N}$ with $2 \le k \le (n + 1)$, k divides $[(n + 1)! + k]$.

    (d) Use the result of Exercise (15c) to prove that for each $n \in \mathbb{N}$, there exist at least n consecutive composite natural numbers.
16. The Twin Prime Conjecture states that there are infinitely many twin primes, but it is not known if this conjecture is true or false. The answers to the following questions, however, can be determined.

    (a) How many pairs of primes p and q exist where $q - p = 3$? That is, how many pairs of primes are there that differ by 3? Prove that your answer is correct. (One such pair is 2 and 5.)

    (b) How many triplets of primes of the form p, $p + 2$, and $p + 4$ are there? That is, how many triplets of primes exist where each prime is 2 more than the preceding prime? Prove that your answer is correct. Notice that one such triplet is 3, 5, and 7.

    Hint: Try setting up cases using congruence modulo 3.
17. Prove the following proposition:

    Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, if $\gcd(a, n) = 1$, then for every $b \in \mathbb{Z}$, there exists an $x \in \mathbb{Z}$ such that $ax \equiv b \pmod{n}$.

    Hint: One way is to start by writing 1 as a linear combination of a and n.
18. Prove the following proposition:

    For all natural numbers m and n, if m and n are twin primes other than the pair 3 and 5, then 36 divides $mn + 1$ and $mn + 1$ is a perfect square.

    Hint: Look at several examples of twin primes. What do you notice about the number that is between the two twin primes? Set up cases based on this observation.

Explorations and Activities

19. **Square Roots and Irrational Numbers.** In Chapter 3, we proved that some square roots (such as $\sqrt{2}$ and $\sqrt{3}$) are irrational numbers. In this activity, we will use the Fundamental Theorem of Arithmetic to prove that if a natural number is not a perfect square, then its square root is an irrational number.

(a) Let n be a natural number. Use the Fundamental Theorem of Arithmetic to explain why if n is composite, then there exist prime numbers $p_1, p_2, ..., p_r$ and natural numbers $\alpha_1, \alpha_2, ..., \alpha_r$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}. \tag{8.2.11}$$

Then,if we use $r = 1$ and $\alpha_1 = 1$ for a prime number, explain why we can write any natural number in the form given in equation (8.2.11).

(b) A natural number b is a perfect square if and only if there exists a natural number a such that $b = a^2$. Explain why 36, 400, and 15876 are perfect squares. Then determine the prime factorization of these perfect squares. What do you notice about these prime factorizations?

(c) Let n be a natural number written in the form given in equation (8.2.11) in part (a). Prove that n is a perfect square if and only if for each natural number k with $1 \le k \le r$, α_k is even.

(d) Prove that for all natural numbers n, if n is not a perfect square, then $\sqrt{n}$ is an irrational number. **Hint**: Use a proof by contradiction.

Answer

Add texts here. Do not delete this text first.

This page titled 8.2: Prime Numbers and Prime Factorizations is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

8.3: Linear Diophantine Equations

? Preview Activity $8.3.1$: Integer Solutions for Linear Equations in One Variable

1. Does the linear equation $6x = 42$ have a solutions that is an integer? Explain.
2. Does the linear equation $7x = -21$ have a solution that is an integer? Explain.
3. Does the linear equation $4x = 9$ have a solution that is an integer? Explain.
4. Does the linear equation $-3x = 20$ have a solution that is an integer? Explain.
5. Prove the following theorem:

Theorem 8.18

Let $a, b \in \mathbb{Z}$ with $a \neq 0$.

- If a divides b, then the equation $ax = b$ has exactly one solution that is an integer.
- If a does not divide b, then the equation $ax = b$ has no solution that is an integer.

? Preview Activity $8.3.2$: Linear Equations in Two Variables

1. Find integers x and y so that $2x + 6y = 25$ or explain why it is not possible to find such a pair of integers.
2. Find integers x and y so that $6x - 9y = 100$ or explain why it is not possible to find such a pair of integers.
3. Notice that $x = 2$ and $y = 1$ is a solution of the equation $3x + 5y = 11$, and that $x = 7$ and $y = -2$ is also a solution of the equation $3x + 5y = 11$.

(a) Find two pairs of integers x and y so that $x > 7$ and $3x + 5y = 11$. (Try to keep the integer values of x as small as possible.)
(b) Find two pairs of integers x and y so that $x < 2$ and $3x + 5y = 11$. (Try to keep the integer values of x as close to 2 as possible.)
(c) Determine formulas (one for x and one for y) that will generate pairs of integers x and y so that $3x + 5y = 11$.
Hint: The two formulas can be written in the form $x = 2 + km$ and $y = 1 + kn$, where k is an arbitrary integer and m and n are specific integers.

4. Notice that $x = 4$ and $y = 0$ is a solution of the equation $4x + 6y = 16$, and that $x = 7$ and $y = -2$ is a solution of the equation $4x + 6y = 16$. (a) Find two pairs of integers x and y so that $x > 7$ and $4x + 6y = 16$. (Try to keep the integer values of x as small as possible.)
   (b) Find two pairs of integers x and y so that $x < 4$ and $4x + 6y = 16$. (Try to keep the integer values of x as close to 4 as possible.)
   (c) Determine formulas (one for x and one for y) that will generate pairs of integers x and y so that $4x + 6y = 16$.
   Hint: The two formulas can be written in the form $x = 4 + km$ and $y = 0 + kn$, where k is an arbitrary integer and m and n are specific integers.

In the two preview activities, we were interested only in integer solutions for certain equations. In such instances, we give the equation a special name.

Definition: Diophantine equation

An equation whose solutions are required to be integers is called a *Diophantine equation.*

Diophantine equations are named in honor of the Greek mathematician Diophantus of Alexandria (circa 300 c.e.). Very little is known about Diophantus' life except that he probably lived in Alexandria in the early part of the fourth centuryc.e. and was probably the first to use letters for unknown quantities in arithmetic problems. His most famous work, Arithmetica, consists of approximately 130 problems and their solutions. Most of these problems involved solutions of equations in various numbers of variables. It is interesting to note that Diophantus did not restrict his solutions to the integers but recognized rational number solutions as well. Today, however, the solutions for a so-called Diophantine equation must be integers.

Definition: linear Diophantine equation in one variable

If a and b are integers with $a \neq 0$, then the equation $ax = b$ is a *linear Diophantine equation in one variable.*

Theorem 8.18 in Preview Activity $8.3.1$ provides us with results that allows us to determine which linear diophantine equations in one variable have solutions and which ones do not have a solution.

A linear Diophantine equation in two variables can be defined in a manner similar to the definition for a linear Diophantine equation in one variable.

Definition: linear Diophantine equation in two variables

Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. The Diophantine equation $ax + by = c$ is called a *linear Diophantine equation in two variables.*

The equations that were investigated in Preview Activity $8.3.2$ were linear Diophantine equations in two variables. The problem of determining all the solutions of a linear Diophantine equation has been completely solved. Before stating the general result, we will provide a few more examples.

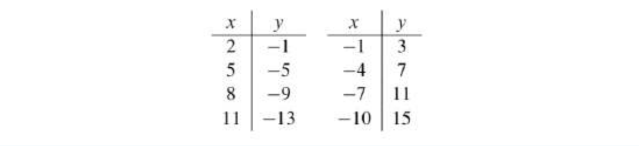
Example 8.19: A Linear Diophantine Equation in Two Variables

The following example is similar to the examples studied in Preview Activity $8.3.2$.

We can use substitution to verify that $x = 2$ and $y = -1$ is a solution of the linear Diophantine equation

$$4x + 3y = 5.$$

The following table shows other solutions of this Diophantine equation.



x	y	x	y
2	−1	−1	3
5	−5	−4	7
8	−9	−7	11
11	−13	−10	15

It would be nice to determine the pattern that these solutions exhibit. If we consider the solution $x = 2$ and $y = -1$ to be the "starting point," then we can see that the other solutions are obtained by adding 3 to x and subtracting 4 from y in the previous solution. So we can write these solutions to the equation as

$$x = 2 + 3k \text{ and } y = -1 - 4k,$$

where k is an integer. We can use substitution and algebra to verify that these expressions for x and y give solutions of this equation as follows:

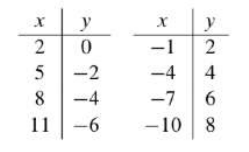
$$\begin{aligned} 4x + 3y &= 4(2 + 3k) + 3(-1 - 4k) \\ &= (8 + 12k) + (-3 - 12k) \\ &= 5. \end{aligned} \tag{8.3.1}$$

We should note that we have not yet proved that these solutions are all of the solutions of the Diophantine equation $4x + 3y = 5$. This will be done later.

If the general form for a linear Diophantine equation is $ax + by = c$, then for this example, $a = 4$ and $b = 3$. Notice that for this equation, we started with one solution and obtained other solutions by adding $b = 3$ to x and subtracting $a = 4$ from y in the previous solution. Also, notice that gcd(3, 4) = 1.

Progress Check 8.20: An Example of a Linear Diophantine Equation

1. Verify that the following table shows some solutions of the linear Diophantine equation $6x + 9y = 12$.



x	y	x	y
2	0	−1	2
5	−2	−4	4
8	−4	−7	6
11	−6	−10	8

2. Follow the pattern in this table to determine formulas for x and y that will generate integer solutions of the equation $6x + 9y = 12$. Verify that the formulas actually produce solutions for the equation $6x + 9y = 12$.

Answer

Add texts here. Do not delete this text first.

Progress Check 8.21: Revisiting Preview Activity $8.3.2$

Do the solutions for the linear Diophantine equations in Preview Activity $8.3.2$ show the same type of pattern as the solutions for the linear Diophantine equations in Example 8.19 and Progress Check 8.20? Explain.

Answer

Add texts here. Do not delete this text first.

The solutions for the linear Diophantine equations in Preview Activity $8.3.2$, Example 8.19, and Progress Check 8.20 provide examples for the second part of Theorem 8.22.

Theorem 8.22

Let a, b and c be integers with $a \neq 0$ and $b \neq 0$, and let $d = \gcd(a, b)$.

1. If d does not divide c, then the linear Diophantine equation $ax + by = c$ has no solution.
2. If d divides c, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if (x_0, y_0) is a particular solution of this equation, then all the solutions of this equation can be written in the form

$$x = x_0 + \frac{b}{d}k \qquad \text{and} \qquad y = y_0 - \frac{a}{d}k, \tag{8.3.2}$$

for some integer k.

Proof

The proof of Part (1) is Exercise (1). For Part (2), we let a, b, and c be integers with $a \neq 0$ and $b \neq 0$, and let $d = \gcd(a, b)$. We also assume that $d \mid c$. Since $d = \gcd(a, b)$, Theorem 8.8 tells us that d is a linear combination of a and b. So there exist integers s and t such that

$$d = as + bt. \tag{8.3.3}$$

Since $d \mid c$, there exists an integer m such that $c = dm$. We can now multiply both sides of equation (8.3.3) by m and obtain

$$\begin{aligned} dm &= (as + bt)m \\ c &= a(sm) + b(tm). \end{aligned} \tag{8.3.4}$$

This means that $x = sm$, $y = tm$ is a solution of $ax + by = c$, and we have proved that the Diophantine equation $ax + by = c$ has at least one solution.

Now let $x = x_0, y = y_0$ be any particular solution of $ax + by = c$, let $k \in \mathbb{Z}$, and let

$$x = x_0 + \frac{b}{d}k \qquad y = y_0 - \frac{a}{d}k. \tag{8.3.5}$$

We now verify that for each $k \in \mathbb{Z}$, the equations in (8.3.4) produce a solution of $ax + by = c$.

$$\begin{aligned} ax+by &= a(x_0+\frac{b}{d}k)+b(y_0-\frac{a}{d}k) \\ &= ax_0+\frac{ab}{d}k+by_0-\frac{ab}{d}k \\ &= ax_0+by_0 \\ &= c. \end{aligned} \tag{8.3.6}$$

This proves that the Diophantine equation $ax+by=c$ has infinitely many solutions.

We now show that every solution of this equation can be written in the form described in (8.3.4). So suppose that x and y are integers such that $ax+by=c$. Then

$$(ax+by)-(ax_0+by_0)=c-c=0,$$

and this equation can be rewritten in the following form:

$$a(x-x_0)=b(y_0-y). \tag{8.3.7}$$

Dividing both sides of this equation by d, we obtain

$$(\frac{a}{d})(x-x_0)=(\frac{b}{d})(y_0-y).$$

This implies that

$\frac{a}{d}$ divides $(\frac{b}{d})(y_0-y)$.

However, by Exercise (7) in Section 8.2, $textgcd(\frac{a}{d},\frac{b}{d})=1$, and so by Theorem 8.12, we can conclude that $\frac{a}{d}$ divides y_0-y. This means that there exists an integer k such that $y_0-y=\frac{a}{d}k$, and solving for y gives

$$y=y_0-\frac{a}{d}k.$$

Substituting this value for y in equation (8.3.5) and solving for x yields

$$x=x_0+\frac{b}{d})k.$$

This proves that every solution of the Diophantine equation $ax+by=c$ can be written in the form prescribed in (8.3.4).

The proof of the following corollary to Theorem 8.22 is Exercise (2)

Theorem 8.3.1

Let a, b, and c be integers with $a\neq 0$ and $b\neq 0$.If a and b are relatively prime, then the linear Diophantine equation $ax+by=c$ has infinitely many solutions. In addition, if x_0, y_0 is a particular solution of this equation, then all the solutions of the equation are given by

$$x=x_0+bk\ y=y_0-ak$$

where $k\in\mathbb{Z}$

Progress Check 8.24 (Linear Diophantine Equations)

1. Use the Euclidean Algorithm to verify that gcd.63; 336/ D 21. What conclusion can be made about linear Diophantine equation $63x+336y=40$ using Theorem 8.22? If this Diophantine equation has solutions, write formulas that will generate the solutions.
2. Use the Euclidean Algorithm to verify that gcd.144; 225/ D 9. What conclusion can be made about linear Diophantine equation $144x+225y=27$ using Theorem 8.22? If this Diophantine equation has solutions, write formulas that will generate the solutions.

Answer

Add texts here. Do not delete this text first.

Exercises 8.3

1. Prove Part (1) of Theorem 8.22:

   Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$, and let $d = \gcd(a, b)$. If d does not divide c, then the linear Diophantine equation $ax + by = c$ has no solution.

2. Prove Corollary 8.23.

   Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. If a and b are relatively prime, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if (x_0, y_0) is a particular solution of this equation, then all the solutions of the equation are given by

   $$x = x_0 + bk \qquad y = y_0 - ak, \tag{8.3.8}$$

   where $k \in \mathbb{Z}$.

3. Determine all solutions of the following linear Diophantine equations.

   (a) $9x + 14y = 1$
   (b) $18x + 22y = 4$
   (c) $48x - 18y = 15$
   (d) $12x + 9y = 6$
   (e) $200x + 49y = 10$
   (f) $200x + 54y = 21$
   (g) $10x - 7y = 31$
   (h) $12x + 18y = 6$
4. A certain rare artifact is supposed to weigh exactly 25 grams. Suppose that you have an accurate balance scale and 500 each of 27 gram weights and 50 gram weights. Explain how to use Theorem 8.22 to devise a plan to check the weight of this artifact.

   Hint: Notice that gcd(50, 27) = 1. Start by writing 1 as a linear combination of 50 and 27.

5. On the night of a certain banquet, a caterer offered the choice of two dinners, a steak dinner for \$25 and a vegetarian dinner for \$16. At the end of the evening, the caterer presented the host with a bill (before tax and tips) for \$1461. What is the minimum number of people who could have attended the banquet? What is the maximum number of people who could have attended the banquet?
6. The goal of this exercise is to determine all (integer) solutions of the linear Diophantine equation in three variables $12x_1 + 9x_2 + 16x_3 = 20$.

   (a) First, notice that gcd(12, 9) = 3. Determine formulas that will generate all solutions for the linear Diophantine equation $3y + 16x_3 = 20$.
   (b) Explain why the solutions (for x_1 and x_2) of the Diophantine equation $12x_1 + 9x_2 = 3y$ can be used to geneate solutions for $12x_1 + 9x_2 + 16x_3 = 20$.
   (c) Use the general value for y from Exercise (6a) to determine the solutions of $12x_1 + 9x_2 = 3y$
   (d) Use the results from Exercises (6a) and (6c) to determine formulas that will generate all solutions for the Diophantine equation $12x_1 + 9x_2 + 16x_3 = 20$.
   Note: These formulas will involve two arbitrary integer parameters. Substitute specific values for these integers and then check the resulting solution in the original equation. Repeat this at least three times.
   (e) Check the general solution for $12x_1 + 9x_2 + 16x_3 = 20$ from Exercise (6d).
7. Use the method suggested in Exercise (6) to determine formulas that will generate all solutions of the Diophantine equation $8x_1 + 4x_2 - 6x_3 = 6$. Check the general solution.
8. Explain why the Diophantine equation $24x_1 - 18x_2 + 60x_3 = 21$ has no solution.
9. The purpose of this exercise will be to prove that the nonlinear Diophantine equation $3x^2 - y^2 = -2$ has no solution.

   (a) Explain why if there is a solution of the Diophantine equation $3x^2 - y^2 = -2$, then that solution must also be a solution

of the congruence $3x^2 - y^2 \equiv -2$ (mod 3).
(b) If there is a solution to the congruence $3x^2 - y^2 \equiv -2$ (mod 3), explain why there then must be an integer y such that $y^2 \equiv 2$ (mod 3).
(c) Use a proof by contradiction to prove that the Diophantine equation $3x^2 - y^2 = -2$ has no solution.

10. Use the method suggested in Exercise (9) to prove that the Diophantine equation $7x^2 + 2 = y^3$ has no solution.

Explorations and Activities

11. **Linear Congruences in One Variable**. Let n be a natural number and let $a, b \in \mathbb{Z}$ with $a \neq 0$. A congruence of the form $ax \equiv b$ (mod n) is called a linear congruence in one variable. This is called a linear congruence since the variable x occurs to the first power.

A solution of a linear congruence in one variable is defined similarly to the solution of an equation. A solution is an integer that makes the resulting congruence true when the integer is substituted for the variable x. For example,

- The integer $x = 3$ is a solution for the congruence $2x \equiv 1$ (mod 5) since $2 \cdot 3 \equiv 1$ (mod 5) is a true congruence.
- The integer $x = 7$ is a solution for the congruence $3x \equiv 1$ (mod 6) since $3 \cdot 7 \equiv 1$ (mod 6) is not a true congruence.

(a) Verify that $x = 2$ and $x = 5$ are the only solutions the linear congruence $4x \equiv 2$ (mod 6) with $0 \leq x < 6$.
(b) Show that the linear congruence $4x \equiv 3$ (mod 6) has no solutions with $0 \leq x < 6$.
(c) Determine all solutions of the linear congruence $3x \equiv 7$ (mod 8) with $0 \leq x < 8$.

The following parts of this activity show that we can use the results of Theorem 8.22 to help find all solutions of the linear congruence $6x \equiv 4$ (mod 8).

(d) Verify that $x = 2$ and $x = 5$ are the only solutions the linear congruence $6x \equiv 4$ (mod 8) with $0 \leq x < 8$.
(e) Use the definition of “congruence” to rewrite the congruence $6x \equiv 4$ (mod 8) in terms of "divides".
(f) Use the definition of “divides” to rewrite the result in part (11e) in the form of an equation. (An existential quantifier must be used.)
(g) Use the results of parts (11d) and (11f) to write an equation that will generate all the solutions of the linear congruence $6x \equiv 4$ (mod 8).
Hint: Use Theorem 8.22. This can be used to generate solutions for x and the variable introduced in part (11f). In this case, we are interested only in the solutions for x.

Now let n be a natural number and let $a, c \in \mathbb{Z}$ with $a \neq 0$. A general linear congruence of the form $ax \equiv c$ (mod n) can be handled in the same way that we handled in $6x \equiv 4$ (mod 8).

(h) Use the definition of “congruence” to rewrite $ax \equiv c$ (mod n) in terms of “divides.”
(i) Use the definition of “divides” to rewrite the result in part (11h) in the form of an equation. (An existential quantifier must be used.)
(j) Let $d = \gcd(a, n)$. State and prove a theorem about the solutions of the linear congruence $ax \equiv c$ (mod n) in the case where d does not divide c.
Hint: Use Theorem 8.22.
(k) Let $d = \gcd(a, n)$. State and prove a theorem about the solutions of the linear congruence $ax \equiv c$ (mod n) in the case where d divides c.

Answer

Add texts here. Do not delete this text first.

This page titled 8.3: Linear Diophantine Equations is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

8.S: Topics in Number Theory (Summary)

Important Definitions

- Greatest common divisor of two integers, page 414
- Linear combination of two integers, page 423
- Prime number, page 426
- Composite number, page 426
- Prime factorization, page 427
- Relatively prime integers, page 428
- Diophantine equation, page 441
- Linear Diophantine equation in two variables, page 441

Important Theorems and Results about Relations, Equivalence Relations, and Equivalence Classes

- **Theorem 8.3**. Let a and b be integers with $a \neq 0$ and $b > 0$. Then gcd(a, b) is the only natural number d such that

  (a) d divides a,
  (b) d divides b, and
  (c) if k is an integer that divides both a and b, then k divides d.
- **Theorem 8.8.** Let a and b be integers, not both 0. Then gcd(a, b) can be written as a linear combination of a and b. That is, there exist integers u and v such that gcd(a, b) $= au + bv$.
- **Theorem 8.9.**
  1. The greatest common divisor, d, is a linear combination of a and b. That is, there exist integers m and n such that $d = am + bn$.
  2. The greatest common divisor, d, divides every linear combination of a and b. That is, for all $x, y \in \mathbb{Z}$, $d \mid (ax + by)$.
  3. The greatest common divisor, d, is the smallest positive number that is a linear combination of a and b.
- **Theorem 8.11**. Let a and b be nonzero integers, and let p be a prime number.
  1. If a and b are relatively prime, then there exist integers m and n such that $am + bn = 1$. That is, 1 can be written as linear combination of a and b.
  2. If $p \mid a$,then $\gcd(a, p) = p$.
  3. If p does not divide a, then $\gcd(a, p) = 1$.
- **Theorem 8.12** Let a, b, and c be integers. If a and b are relatively prime and $a \mid (bc)$, then $a \mid c$.
- **Corollary8.14**
  1. Let $a, b \in \mathbb{Z}$, and let p be a prime number. If $p \mid (ab)$, then $p \mid a$ or $p \mid b$.
  2. Let p be a prime number, let $n \in \mathbb{N}$, and let $a_1, a_2, ..., a_n \in \mathbb{Z}$. If $p \mid (a_1 a_2 \cdots a_n)$, then there exists a natural number k with $1 \leq k \leq n$ such that $p \mid a_k$.
- **Theorem 8.15, The Fundamental Theorem of Arithmetic**
  1. Each natural number greater than 1 is either a prime number or is a product of prime numbers.
  2. Let $n \in \mathbb{N}$ with $n > 1$. Assume that

$$n = p_1 p_2 \cdots p_r \text{ and that } n = q_1 q_2 \cdots q_s. \tag{8.S.1}$$

  where $p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_s$ are primes with $p_1 \leq p_2 \leq \cdots p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$. Then $r = s$, and for each j from 1 to r, $p_j = q_j$.

- **Theorem 8.16.** There are infinitely many prime numbers.
- **Theorem 8.22.** Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$, and let $d = \gcd(a, b)$.

  1. If d does not divide c, then the linear Diophantine equation $ax + by = c$ has no solution.

  2. If d divides c, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if (x_0, y_0) is a particular solution of this equation, then all the solutions of the equation are given by

$$x = x_0 + \frac{b}{d}k \quad \text{and} \quad y = y_0 - \frac{a}{d}k. \tag{8.S.2}$$

where $k \in \mathbb{Z}$.

- **Corollary8.23.** Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. If a and b are relatively prime, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if x_0, y_0 is a particular solution of this equation, then all the solutions of the equation are given by

$$x = x_0 + bk \quad \text{and} \quad y = y_0 - ak, \tag{8.S.3}$$

page468image4254810384page468image4254810656page468image4254810928

where $k \in \mathbb{Z}$.

This page titled 8.S: Topics in Number Theory (Summary) is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

CHAPTER OVERVIEW

9: Finite and Infinite Sets

9.1: Finite Sets
9.2: Countable Sets
9.3: Uncountable Sets
9.S: Finite and Infinite Sets (Summary)

This page titled 9: Finite and Infinite Sets is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

9.1: Finite Sets

Preview Activity $9.1.1$: Equivalent Sets, Part 1

1. Let A and B be sets and let f be a function from A to B. ($f : A \to B$). Carefully complete each of the following using appropriate quantifiers: (If necessary, review the material in Section 6.3.)
   a. The function f is an injection provided that...
   b. The function f is not an injection provided that...
   c. The function f is a surjection provided that...
   d. The function f is not a surjection provided that...
   e. The function f is a bijection provided that...

Definitions: equivalent Sets and one-to-one correspondence

Let A and B be sets.

- The set A is **equivalent** to the set B provided that there exists a bijection from the set A onto the set B. In this case, we write $A \approx B$.
- When $A \approx B$, we also say that the set A is in **one-to-one correspondence** with the set B and that the set A has the same **cardinality** as the set B.

Note: When A is not equivalent to B, we write $A \not\approx B$.

2. For each of the following, use the definition of equivalent sets to determine if the first set is equivalent to the second set.
   a. $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$
   b. $C = \{1, 2\}$ and $B = \{a, b, c\}$
   c. $X = \{1, 2, 3, ..., 10\}$ and $Y = \{57, 58, 59, ..., 66\}$
3. Let D^+ be the set of all odd natural numbers. Prove that the function $f : \mathbb{N} \to D^+$ defined by $f(x) = 2x - 1$, for all $x \in \mathbb{N}$, is a bijection and hence that $N \approx D^+$.
4. Let $\mathbb{R}^+$ be the set of all positive real numbers. Prove that the function $g : \mathbb{R} \to \mathbb{R}^+$ defined by $g(x) = e^x$, for all $x \in \mathbb{R}$ is a bijection and hence, that $\mathbb{R} \approx \mathbb{R}^+$.

Preview Activity $9.1.2$: Equivalent Sets, Part 2

1. Review Theorem 6.20 in Section 6.4, Theorem 6.26 in Section 6.5, and Exercise (9) in Section 6.5.
2. Prove each part of the following theorem.

Theorem 9.1.

Let A, B, and C be sets.

a. For each set A, $A \approx A$.
b. For all sets A and B, if $A \approx B$, then $B \approx A$.
c. For all sets A, B and C, if $A \approx B$ and $B \approx C$, then $A \approx C$.

Equivalent Sets

In Preview Activity $9.1.1$, we introduced the concept of equivalent sets. The motivation for this definition was to have a formal method for determining whether or not two sets "have the same number of elements." This idea was described in terms of a one-to-one correspondence (a bijection) from one set onto the other set. This idea may seem simple for finite sets, but as we will see, this idea has surprising consequences when we deal with infinite sets. (We will soon provide precise definitions for finite and infinite sets.)

Technical Note

The three properties we proved in Theorem 9.1 in Preview Activity 9.1.2 are very similar to the concepts of reflexive, symmetric, and transitive relations. However, we do not consider equivalence of sets to be an equivalence relation on a set U since an equivalence relation requires an underlying (universal) set U. In this case, our elements would be the sets A, B, and C, and these would then have to subsets of some universal set W (elements of the power set of W). For equivalence of sets, we are not requiring that the sets A, B, and C be subsets of the same universal set. So we do not use the term relation in regards to the equivalence of sets. However, if A and B are sets and $A \approx B$, then we often say that A and B are equivalent sets.

Progress Check 9.2: Examples of Equivalent Sets

We will use the definition of equivalent sets from in Preview Activity 9.1.1 in all parts of this progress check. It is no longer sufficient to say that two sets are equivalent by simply saying that the two sets have the same number of elements.

1. Let $A = \{1, 2, 3, ..., 99, 100\}$ and let $B = \{351, 352, 353, ..., 449, 450\}$. Define $f : A \to B$ by $f(x) = x + 350$, for each x in A.
   Prove that f is a bijection from the set A to the set B and hence, $A \approx B$.
2. Let E be the set of all even integers and let D be the set of all odd integers.
   Prove that $E \approx D$ by proving that $F : E \to D$, where $F(x) = x + 1$, for all $x \in E$, is a bijection.
3. Let (0, 1) be the open interval of real numbers between 0 and 1. Similarly, if $b \in \mathbb{R}$ with $b > 0$, let $0, b$ be the open interval of real numbers between 0 and b.
   Prove that the function $f : (0, 1) \to (0, b)$ by $f(x) = bx$, for all $x \in (0, 1)$, is a bijection and hence $(0, 1) \approx (0, b)$.

Answer

Add texts here. Do not delete this text first.

In Part (3) of Progress Check 9.2, notice that if $b > 1$, then (0, 1) is a proper subset of (0, b) and $(0, 1) \approx (0, b)$. Also, in Part (3) of Preview Activity 9.1.1, we proved that the set D of all odd natural numbers is equivalent to $\mathbb{N}$, and we know that D is a proper subset of $\mathbb{N}$.

These results may seem a bit strange, but they are logical consequences of the definition of equivalent sets. Although we have not defined the terms yet, we will see that one thing that will distinguish an infinite set from a finite set is that an infinite set can be equivalent to one of its proper subsets, whereas a finite set cannot be equivalent to one of its proper subsets.

Finite Sets

In Section 5.1, we defined the **cardinality** of a finite set A, denoted by card(A), to be the number of elements in the set A. Now that we know about functions and bijections, we can define this concept more formally and more rigorously. First, for each $k \in \mathbb{N}$, we define $\mathbb{N}_k$ to be the set of all natural numbers between 1 and k, inclusive. That is,

$$\mathbb{N}_k = \{1, 2, ..., k\}.$$

We will use the concept of **equivalent sets** introduced in Preview Activity 9.1.1 to define a finite set.

Definition: finite and infinite sets

- A set A is a **finite set** provided that $A = \emptyset$ or there exists a natural number k such that $A \approx \mathbb{N}_k$.
- A set is an **infinite set** provided that it is not a finite set.
- If $A \approx \mathbb{N}_k$, we say that the set A has **cardinality** k (or **cardinal number** k), and we write card(A) $= k$.

In addition, we say that the empty set has **cardinality 0** (or **cardinal number 0**), and we write $\text{card}(\emptyset) = 0$.

Notice that by this definition, the empty set is a finite set. In addition, for each $k \in \mathbb{N}$, the identity function on $\mathbb{N}_k$ is a bijection and hence, by definition, the set $\mathbb{N}_k$ is a finite set with cardinality k.

Theorem 9.3

Any set equivalent to a finite nonempty set A is a finite set and has the same cardinality as A.

Proof

Suppose that A is a finite nonempty set, B is a set, and $A \approx B$. Since A is a finite set, there exists a $k \in \mathbb{N}$ such that $A \approx \mathbb{N}_k$. We also have assumed that $A \approx B$ and so by part (b) of Theorem 9.1 (in Preview Activity 9.1.2), we can conclude that $B \approx A$. Since $A \approx \mathbb{N}_k$, we can use part (c) of Theorem 9.1 to conclude that $B \approx \mathbb{N}_k$. Thus, B is finite and has the same cardinality as A.

It may seem that we have done a lot of work to prove an “obvious” result in Theorem 9.3. The same may be true of the remaining results in this section, which give further results about finite sets. One of the goals is to make sure that the concept of cardinality for a finite set corresponds to our intuitive notion of the number of elements in the set. Another important goal is to lay the groundwork for a more rigorous and mathematical treatment of infinite sets than we have encountered before. Along the way, we will see the mathematical distinction between finite and infinite sets.

The following two lemmas will be used to prove the theorem that states that every subset of a finite set is finite.

Lemma 9.4

If A is a finite set and $x \notin A$, then $A \cup \{x\}$ is a finite set and $\text{card}(A \cup \{x\}) = \text{card}(A) + 1$.

Proof

Let A is a finite set and assume that $\text{card}(A) = k$, where $k = 0$ or $k \in \mathbb{N}$. Assume $x \notin A$.

If $A = \emptyset$, then $\text{card}(A) = 0$ and $A \cup \{x\} = \{x\}$, which is equivalent to $\mathbb{N}_1$. Thus, $A \cup \{x\}$ is a finite set with cardinality 1, which equals card(A) + 1.

If $A \neq \emptyset$, then $A \approx \mathbb{N}_k$, for some $k \in \mathbb{N}$. This means that $\text{card}(A) = k$, and there exists a bijection $f : A \to \mathbb{N}_k$. We will now use this bijection to define a function $g : A \cup \{x\} \to \mathbb{N}_{k+1}$ and then prove that the function g is a bijection. We define $g : A \cup \{x\} \to \mathbb{N}_{k+1}$ as follows: For each $t \in A \cup \{x\}$,

$$g(t) = \begin{cases} f(t) & \text{if } t \in A \\ k+1 & \text{if } t = x. \end{cases}$$

To prove that g is an injection, we let $x_1, x_2 \in A \cup \{x\}$ and assume $x_1 \neq x_2$.

- If $x_1, x_2 \in A$, then since f is a bijection, $f(x_1) \neq f(x_2)$, and this implies that $g(x_1) \neq g(x_2)$.
- If $x_1 = x$, then since $x_2 \neq x_1$, we conclude that $x_2 \neq x$ and hence $x_2 \in A$. So $g(x_1) = k + 1$, and since $f(x_2) \in \mathbb{N}_k$ and $g(x_2) = f(x_2)$, we can conclude that $g(x_1) \neq g(x_2)$.

This proves that the function g is an injection. The proof that g is a surjection is Exercise (1). Since g is a bijection, we conclude that $A \cup \{x\} \approx \mathbb{N}_{k+1}$, and

$$\text{card}(A \cup \{x\}) = k + 1.$$

Since $\text{card}(A) = k$, we have proved that $\text{card}(A \cup \{x\}) = \text{card}(A) + 1$.

Lemma 9.5

For each natural number m, if $A \subseteq \mathbb{N}_m$, then A is a finite set and $\text{card}(A) \leq m$.

Proof

We will use a proof using induction on m. For each $m \in \mathbb{N}$, let $P(m)$ be, "If $A \subseteq \mathbb{N}_m$, then A is finite and $\text{card}(A) \leq m$".

We first prove that $P(1)$ is true. If $A \subseteq \mathbb{N}_1$, then $A = \emptyset$ or $A = \{1\}$, both of which are finite and have cardinality less than or equal to the cardinality of $\mathbb{N}_1$. This proves that $P(1)$ is true.

For the inductive step, let $k \in \mathbb{N}$ and assume that $P(k)$ is true. That is, assume that if $B \subseteq \mathbb{N}_k$, then B is a finite set and $\text{card}(B) \leq k$. We need to prove that $P(k+1)$ is true.

So assume that A is a subset of $\mathbb{N}_{k+1}$. Then $A - \{k+1\}$ is a subset of $\mathbb{N}_k$. Since $P(k)$ is true, $A - \{k+1\}$ is a finite set and

$$\text{card}(A - \{k+1\}) \leq k.$$

There are two cases to consider: Either $k+1 \in A$ or $k+1 \notin A$.

If $k+1 \notin A$, then $A = A - \{k+1\}$. Hence, A is finite and

$$\text{card}(A) \leq k < k+1.$$

If $k+1 \in A$, then $A = (A - \{k+1\}) \cup \{k+1\}$. Hence, by Lemma 9.4, A is a finite set and

$$\text{card}(A) = \text{card}(A - \{k+1\} + 1\backslash).$$

Since $\text{card}(A - \{k+1\}) \leq k$, we can conclude that $\text{card}(A) \leq k+1$.

This means that we have proved the inductive step. Hence, by mathematical induction, for each $m \in \mathbb{N}$, if $A \subset \mathbb{N}_m$, then A is finite and $\text{card}(A) \leq m$.

The preceding two lemmas were proved to aid in the proof of the following theorem.

Theorem 9.6.

If S is a finite set and A is a subset of S, then A is a finite set and $\text{card}(A) \leq \text{card}(S)$.

Proof

Let S be a finite set and assume that A is a subset of S. If $A = \emptyset$, then A is a finite set and $\text{card}(A) \leq \text{card}(S)$. So we assume that $A \neq \emptyset$.

Since S is finite, there exists a bijection $f : S \to \mathbb{N}_k$ for some $k \in \mathbb{N}$. In this case, $\text{card}(S) = k$. We need to show that A is equivalent to a finite set. To do this, we define $g : A \to f(A)$ by

$$g(x) = f(x) \text{ for each } x \in A.$$

Since f is an injection, we conclude that g is an injection. Now let $y \in f(A)$. Then there exists an $a \in A$ such that $f(a) = y$. But by the definition of g, this means that $g(a) = y$, and hence g is a surjection. This proves that g is a bijection.

Hence, we have proved that $A \approx f(A)$. Since $f(A)$ is a subset of $\mathbb{N}_k$, we use Lemma 9.5 to conclude that $f(A)$ is finite and $\text{card}(f(A)) \leq k$. In addition, by Theorem 9.3, A is a finite set and $\text{card}(A) = \text{card}(f(A))$. This proves that A is a finite set and $\text{card}(A) \leq \text{card}(S)$.

Lemma 9.4 implies that adding one element to a finite set increases its cardinality by 1. It is also true that removing one element from a finite nonempty set reduces the cardinality by 1. The proof of Corollary 9.7 is Exercise (4).

corollary 9.7

If A is a finite set and $x \in A$, then $A - \{x\}$ is a finite set and $\text{card}(A - \{x\}) = \text{card}(A) - 1$

The next corollary will be used in the next section to provide a mathematical distinction between finite and infinite sets.

Corollary 9.8

A finite set is not equivalent to any of its proper subsets.

Proof

Let B be a finite set and assume that A is a proper subset of B. Since A is a proper subset of B, there exists an element x in $B - A$. This means that A is a subset of $B - \{x\}$. Hence, by Theorem 9.6,

$$\text{card}(A) \leq \text{card}(B - \{x\}).$$

Also, by Corollary 9.7

$$\text{card}(B - \{x\}) = \text{card}(B) - 1.$$

Hence, we may conclude that $\text{card}(A) \le \text{card}(B) - 1$ and that

$$\text{card}(A) < \text{card}(B).$$

Theorem 9.3 implies that $B \not\approx A$. This proves that a finite set is not equivalent to any of its proper subsets.

The Pigeonhole Principle

The last property of finite sets that we will consider in this section is often called the **Pigeonhole Principle**. The "pigeonhole" version of this property says, "If m pigeons go into r pigeonholes and $m > r$, then at least one pigeonhole has more than one pigeon."

In this situation, we can think of the set of pigeons as being equivalent to a set P with cardinality m and the set of pigeonholes as being equivalent to a set H with cardinality r. We can then define a function $f : P \to H$ that maps each pigeon to its pigeonhole. The Pigeonhole Principle states that this function is not an injection. (It is not one-to-one since there are at least two pigeons "mapped" to the same pigeonhole.)

Theorem 9.9: The Pigeonhole Principle

Let A and B be finite sets. If $\text{card}(A) > \text{card}(B)$, then any function $f : A \to B$ is not an injection.

Proof

Let A and B be finite sets. We will prove the contrapositive o the theorem, which is, if there exists a function $f : A \to B$ that is an injection, then $\text{card}(A) \le \text{card}(B)$.

So assume that $f : A \to B$ is an injection. As in Theorem 9.6, we define a function $g : A \to f(A)$ by

$$g(x) = f(x) \text{ for each } x \in A.$$

As we saw in Theorem 9.6, the function g is a bijection. But then $A \approx f(A)$ and $f(A) \subseteq B$. Hence,

$\text{card}(A) = \text{card}(f(x))$ and $\text{card} f((A)) \le \text{card}(B)$.

Hence, $\text{card} f((A)) \le \text{card}(B)$, and this proves the contrapositive. Hence, if $\text{card}(A) > \text{card}(B)$, then any function $f : A \to B$ is not an injection.

The Pigeonhole Principle has many applications in the branch of mathematics called "combinatorics." Some of these will be explored in the exercises.

Exercises 9.1

1. Prove that the function $g : A \cup \{x\} \to \mathbb{N}_{k+1}$ in Lemma 9.4 is a surjection.
2. Let A be a subset of some universal set U. Prove that if $x \in U$, then $A \times \{x\} \approx A$.
3. Let E^+ be the set of all even natural numbers. Prove that $\mathbb{N} \approx E^+$.
4. Prove Corollary 9.7.
   If A is a finite set and $x \in A$, then $A - \{x\}$ is a finite set and $\text{card}(A - \{x\}) = \text{card}(A) - 1$
   Hint: One approch is to use the fact that $A = (A - \{x\}) \cup \{x\}$.
5. Let A and B be sets. Prove that

   (a) If A is a finite set, then $A \cap B$ is a finite set.
   (b) If $A \cup B$ is a finite set, then A and B are finite set.
   (c) If $A \cap B$ is an infinite set, then A is an infinite set.
   (d) If A is an infinite set or B is an infinite set, then $A \cup B$ is an infinite set.
6. There are over 7 million people living in New York City. It is also known that the maximum number of hairs on a human head is less than 200,000. Use the Pigeonhole Principle to prove that there are at least two people in the city of New York with the same number of hairs on their heads.

7. Prove the following proposiitons:

   (a) If A, B, C, and D are sets with $A \approx B$ and $C \approx D$, then $A \times C \approx B \times D$.
   (b) If A, B, C, and D are sets with $A \approx B$ and $C \approx D$ and if A and C are disjoint and B and D are disjoint, then $A \cup C \approx B \cup D$.

   Hint: Since $A \approx B$ and $C \approx D$, there exist bijections $f : A \to B$ and $g : C \to D$. To prove that $A \times C \approx B \times D$, prove that $h : A \times C \to B \times D$ is a bijection, where $h(a, c) = (f(a), g(c))$, for all $(a, c) \in A \times C$.
   If $A \cap C = \emptyset$ and $B \cap D = \emptyset$, then to prove that $A \cup C \approx B \cup D$, prove that the following function is a bijection: $k : A \cup C \to B \cup D$, where

   $$k(x) = \begin{cases} f(x) & \text{if } t \in A \\ g(x) & \text{if } x \in C. \end{cases} \tag{9.1.1}$$

8. Let $A = \{a, b, c\}$.

   (a) Construct a function $f : \mathbb{N}_5 \to A$ such that f is a surjection.
   (b) Use the function f to construct a function $g : A \to \mathbb{N}_5$ so that $f \circ g = I_A$, where I_A is the identity function on the set A. Is the function g an injection? Explain.
9. This exercise is a generalization of Exercise (8). Let m be a natural number, let A be a set, and assume that $f : \mathbb{N}_m \to A$ is a surjection. Define $g : A \to \mathbb{N}_m$ asfollows:
   For each $x \in A$, $g(x) = j$, where j is the least natural number in $f^{-1}(\{x\})$.
   Prove that $f \circ g = I_A$, where I_A is the identity function on the set A and prove that g is an injection.
10. Let B be a finite, nonempty set and assume that $f : B \to A$ is a surjection. Prove that there exists a function $h : A \to B$ such that $f \circ h = I_A$ and h is an injection.
    Hint: Since B is finite, there exists a natural number m such that $\mathbb{N}_m \approx B$. This means there exists a bijection $k : \mathbb{N}_m \to B$. Now let $h = k \circ g$, where g is the function constructed in Exercise (9).

    Explorations and Activities
11. **Using the Pigeonhole Principle.** For this activity, we will consider subsets of $\mathbb{N}_3 0$ that contain eight elements.

    (a) One such set is $A = \{3, 5, 11, 17, 21, 24, 26, 29\}$. Notice that

    $$\begin{array}{rcr} \{3, 21, 24, 26\} \subseteq A & \text{and} & 3 + 21 + 24 + 26 = 74 \\ \{3, 5, 11, 26, 29\} \subseteq A & \text{and} & 3 + 5 + 11 + 26 + 29 = 74 \end{array} \tag{9.1.2}$$

    Use this information to find two disjoint subsets of A whose elements have the same sum.
    (b) Let $B = \{3, 5, 9, 12, 15, 18, 21, 24\}$. Find two disjoint subsets of B whose elements have the same sum. Note: By convention, if $T = \{a\}$, where $a \in \mathbb{N}$, then the sum of the elements in T is equal to a.
    (c) Now let C be any subset of $\mathbb{N}_{30}$ that contains eight elements.
    i. How many subsets does C have?
    ii. The sum of the elements of the empty set is 0. What is the maximum sum for any subset of $\mathbb{N}_{30}$ that contains eight elements.? Let M be this maximum sum.
    iii. Now define a function $f : \mathcal{P}(C) \to \mathbb{N}_M$ so that for each $X \in \mathcal{P}$, $f(X)$ is equal to the sum of the elements in X.
    Use the Pigeonhole Principle to prove that there exist two subsets of C whose elements have the same sum.
    (d) If the two subsets in part (11(c)iii) are not disjoint, use the idea presented in part (11a) to prove that there exist two disjoint subsets of C whose elements have the same sum.
    (e) Let S be a subset of $\mathbb{N}_{99}$ that contains 10 elements. Use the Pigeonhole Principle to prove that there exist two disjoint subsets of S whose elements have the same sum.

Answer

Add texts here. Do not delete this text first.

This page titled 9.1: Finite Sets is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

9.2: Countable Sets

Preview Activity 9.2.1: Introduction to Infinite Sets

In Section 9.1, we defined a **finite set** to be the empty set or a set A such that $A \approx \mathbb{N}_k$ for some natural number k. We also defined an **infinite set** to be a set that is not finite, but the question now is, “How do we know if a set is infinite?” One way to determine if a set is an infinite set is to use Corollary 9.8, which states that a finite set is not equivalent to any of its subsets. We can write this as a conditional statement as follows:

> If A is a finite set, then A is not equivalent to any of its proper subsets. or more formally as
>
> For each set A, if A is a finite set, then for each proper subset B of A, $A \not\approx B$.

1. Write the contrapositive of the preceding conditional statement. Then explain how this statement can be used to determine if a set is infinite.
2. Let DC be the set of all odd natural numbers. In Preview Activity 9.2.1 from Section 9.1, we proved that $\mathbb{N} \approx D^+$.

   (a) Use this to explain carefully why $\mathbb{N}$ is an infinite set.
   (b) Is D^+ a finite set or an infinite set? Explain carefully how you know.

3. Let b be a positive real number. Let (0, 1) and $(0, b)$ be the open intervals from 0 to 1 and 0 to b, respectively. In Part (3) of Progress Check 9.2 (on page 454), we proved that $(0, 1) \approx (0, b)$.

   (a) Use a value for b where $0 < b < 1$ to explain why (0, 1) is an infinite set.
   (b) Use a value for b where $b > 1$ to explain why $(0, b)$ is an infinite set.

Preview Activity 9.2.2: A Function from $\mathbb{N}$ to $\mathbb{Z}$

In this preview activity, we will define and explore a function $f : \mathbb{N} \to \mathbb{Z}$. We will start by defining $f(n)$ for the first few natural numbers n.

$$\begin{array}{ll} f(1) = 0 & \\ f(2) = 1 & f(3) = -1 \\ f(4) = 2 & f(5) = -2 \\ f(6) = 3 & f(7) = -3 \end{array}$$

Notice that if we list the outputs of f in the order $f(1)$, $f(2)$, $f(3)$, ..., we create the following list of integers: 0, 1, -1, 2, -2, 3, -3, ... We can also illustrate the outputs of this function with the following diagram:

$$\begin{array}{ccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \cdots \\ 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & -4 & 5 & \cdots \end{array}$$

Figure 9.1: A Function from $\mathbb{N}$ to $\mathbb{Z}$

1. If the pattern suggested by the function values we have defined continues, what are $f(11)$ and $f(12)$? What is $f(n)$ for n from 13 to 16?
2. If the pattern of outputs continues, does the function f appear to be an injection? Does f appear to be a surjection? (Formal proofs are not required.)

   We will now attempt to determine a formula for $f(n)$, where $n \in \mathbb{N}$. We will actually determine two formulas: one for when n is even and one for when n is odd.
3. Look at the pattern of the values of $f(n)$ when n is even. What appears to be a formula for $f(n)$ when n is even?
4. Look at the pattern of the values of $f(n)$ when n is odd. What appears to be a formula for $f(n)$ when n is odd?
5. Use the work in Part (3) and Part (4) to complete the following: Define $f : \mathbb{N} \to \mathbb{Z}$, where

$$f(n) = \begin{cases} ?? & \text{if } n \text{ is even} \\ ?? & \text{if } n \text{ is odd.} \end{cases} \tag{9.2.1}$$

6. Use the formula in Part (5) to (a) Calculate $f(1)$ through $f(10)$. Are these results consistent with the pattern exhibited at the beginning of this preview activity?
   (b) Calculate $f(1000)$ and $f(1001)$.
   (c) Determine the value of n so that $f(n) = 1000$.

In this section, we will describe several infinite sets and define the cardinal number for so-called countable sets. Most of our examples will be subsets of some of our standard numbers systems such as $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$.

Infinite Sets

In Preview Activity $9.2.1$, we saw how to use Corollary 9.8 to prove that a set is infinite. This corollary implies that if A is a finite set, then A is not equivalent to any of its proper subsets. By writing the contrapositive of this conditional statement, we can restate Corollary 9.8 in the following form:

Corollary 9.8

If a set A is equivalent to one of its proper subsets, then A is infinite.

In Preview Activity $9.2.1$, we used Corollary 9.8 to prove that

- The set of natural numbers, $\mathbb{N}$, is an infinite set.
- The open interval (0, 1) is an infinite set.

Although Corollary 9.8 provides one way to prove that a set is infinite, it is sometimes more convenient to use a proof by contradiction to prove that a set is infinite. The idea is to use results from Section 9.1 about finite sets to help obtain a contradiction. This is illustrated in the next theorem.

Theorem 9.10.

Let A and B be sets.

1. If A is infinite and $A \approx B$, then B is infinite.
2. If A is infinite and $A \subseteq B$, then B is infinite.

Proof

We will prove part (1). The proof of part (2) is exercise (3) on page 473.

To prove part (1), we use a proof by contradiction and assume that A is an infinite set, $A \approx B$, and B is not infinite. That is, B is a finite set. Since $A \approx B$ and B is finite, Theorem 9.3 on page 455 implies that A is a finite set. This is a contradiction to the assumption that A is infinite. We have therefore proved that if A is infinite and $A \approx B$, then B is infinite.

Progress Check 9.11 (Examples of Infinite Sets)

1. In Preview Activity $9.2.1$, we used Corollary 9.8 to prove that $\mathbb{N}$ is an infinite set. Now use this and Theorem 9.10 to explain why our standard number systems ($\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$) are infinite sets. Also, explain why the set of all positive rational numbers, $\mathbb{Q}^+$, and the set of all positive real numbers, $\mathbb{R}^+$, are infinite sets.
2. Let D^+ be the set of all odd natural numbers. In Part (2) of Preview Activity $9.2.1$, we proved that $D^+ \approx \mathbb{N}$. Use Theorem 9.10 to explain why D^+ is an infinite set.
3. Prove that the set E^+ of all even natural numbers is an infinite set.

Answer

Add texts here. Do not delete this text first.

Countably Infinite Sets

In Section 9.1, we used the set $\mathbb{N}_k$ as the standard set with cardinality k in the sense that a set is finite if and only if it is equivalent to $\mathbb{N}_k$. In a similar manner, we will use some infinite sets as standard sets for certain infinite cardinal numbers. The first set we will use is $\mathbb{N}$.

We will formally define what it means to say the elements of a set can be "counted" using the natural numbers. The elements of a finite set can be "counted" by defining a bijection (one-to-one correspondence) between the set and $\mathbb{N}_k$ for some natural number k. We will be able to "count" the elements of an infinite set if we can define a one-to-one correspondence between the set and $\mathbb{N}$.

Definition

The **cardinality of** $\mathbb{N}$ is denoted by $\aleph_0$. The symbol $\aleph$ is the first letter of the Hebrew alphabet, **aleph**. The subscript 0 is often read as "naught" (or sometimes as "zero" or "null"). So we write

$$\text{card}(\mathbb{N}) = \aleph_0$$

and say that the cardinality of $\mathbb{N}$ is "aleph naught."

Definition

A set A is **countably infinite** provided that $A \approx \mathbb{N}$. In this case, we write

$$\text{card}(A) = \aleph_0$$

A set that is countably infinite is sometimes called a **denumerable** set. A set is **countable** provided that it is finite or countably infinite. An infinite set that is not countably infinite is called an **uncountable set.**

? progress check 9.12. (examples of countably infinite sets)

1. In Preview Activity $9.2.1$ from Section 9.1, we proved that $\mathbb{N} \approx D^+$, where D^+ is the set of all odd natural numbers. Explain why $\text{card}(D^+) = \aleph_0$.
2. Use a result from Progress Check 9.11 to explain why $\text{card}(E^+) = \aleph_0$.
3. At this point, if we wish to prove a set S is countably infinite, we must find a bijection between the set S and some set that is known to be countably infinite.

   Let S be the set of all natural numbers that are perfect squares. Define a function

   $$f : S \to \mathbb{N} \tag{9.2.2}$$

   that can be used to prove that $S \approx \mathbb{N}$ and, hence, that $\text{card}(S) = \aleph_0$.

Answer

Add texts here. Do not delete this text first.

The fact that the set of integers is a countably infinite set is important enough to be called a theorem. The function we will use to establish that $\mathbb{N} \approx \mathbb{Z}$ was explored in Preview Activity $9.2.2$.

Theorem 9.13

The set $\mathbb{Z}$ of integers is countably infinite, and so $\text{card}(\mathbb{Z}) = \aleph_0$

Proof

To prove that $\mathbb{N} \approx \mathbb{Z}$, we will use the following funciton: $f : \mathbb{N} \to \mathbb{Z}$, where

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ \dfrac{1-n}{2} & \text{if } n \text{ is odd.} \end{cases}$$

From our work in Preview Activity $9.2.2$, it appears that if n is an even natural number, then $f(n) > 0$, and if n is an odd natural number, then $f(n) \le 0$. So it seems reasonable to use cases to prove that f is a surjection and that f is an injection. To prove that f is a surjection, we let $y \in \mathbb{Z}$.

- If $y > 0$, then $2y \in \mathbb{N}$, and

$$f(2y) = \frac{2y}{2} = y. \tag{9.2.3}$$

- If $y \le 0$, then $-2y \ge 0$ and $1-2y$ is an odd natural number. Hence,

$$f(1-2y) = \frac{1-(1-2y)}{2} = \frac{2y}{2} = y. \tag{9.2.4}$$

These two cases prove that if $y \in \mathbb{Z}$, then there exists an $n \in \mathbb{N}$ such that $f(n) = y$. Hence, f is a surjection.

To prove that f is an injection, we let $m, n \in \mathbb{N}$ and assume that $f(m) = f(n)$. First note that if one of m and n is odd and the other is even, then one of $f(m)$ and $f(n)$ is positive and the other is less than or equal to 0. So if $f(m) = f(n)$, then both m and n must be even or both m and n must be odd.

- If both m and n are even, then

$$f(m) = f(n) \text{ implies that } \frac{m}{2} = \frac{n}{2} \tag{9.2.5}$$

  and hence that $m = n$.
- If both m and n are odd, then

$$f(m) = f(n) \text{ implies that } \frac{1-m}{2} = \frac{1-n}{2}. \tag{9.2.6}$$

  From this, we conclude that $1-m = 1-n$ and hence that $m = n$. This proves that if $f(m) = f(n)$, then $m = n$ and hence that f is an injection.

Since f is both a surjection and an injection, we see that f is a bijection and, therefore, $\mathbb{N} \approx \mathbb{Z}$. Hence, $\mathbb{Z}$ is countably infinite and $\text{card}(\mathbb{Z}) = \aleph_0$.

The result in Theorem 9.13 can seem a bit surprising. It exhibits one of the distinctions between finite and infinite sets. If we add elements to a finite set, we will increase its size in the sense that the new set will have a greater cardinality than the old set. However, with infinite sets, we can add elements and the new set may still have the same cardinality as the original set. For example, there is a one-to-one correspondence between the elements of the sets $\mathbb{N}$ and $\mathbb{Z}$. We say that these sets have the same cardinality.

Following is a summary of some of the main examples dealing with the cardinality of sets that we have explored.

- The sets $\mathbb{N}_k$, where $k \in \mathbb{N}$, are examples of sets that are countable and finite.
- The sets $\mathbb{N}$, $\mathbb{Z}$, the set of all odd natural numbers, and the set of all even natural numbers are examples of sets that are countable and countably infinite.
- We have not yet proved that any set is uncountable.

The Set of Positive Rational Numbers

If we expect to find an uncountable set in our usual number systems, the rational numbers might be the place to start looking. One of the main differences between the set of rational numbers and the integers is that given any integer m, there is a next integer, namely $m+1$. This is not true for the set of rational numbers. We know that $\mathbb{Q}$ is closed under division (by nonzero rational numbers) and we will see that this property implies that given any two rational numbers, we can also find a rational number between them. In fact, between any two rational numbers, we can find infinitely many rational numbers. It is this property that may lead us to believe that there are "more" rational numbers than there are integers.

The basic idea will be to "go half way" between two rational numbers. For example, if we use $a = \frac{1}{3}$ and $b = \frac{1}{2}$, we can use

$$\frac{a+b}{2} = \frac{1}{2}(\frac{1}{3} + \frac{1}{2}) = \frac{5}{12}$$

as a rational number between a and b. We can then repeat this process to find a rational number between $\frac{5}{12}$ and $\frac{1}{2}$.

So we will now let a and b be any two rational numbers with $a < b$ and let $c_1 = \dfrac{a+b}{2}$. We then see that

$$\begin{aligned} c_1 - a &= \frac{a+b}{2} - a \\ &= \frac{a+b}{2} - \frac{2a}{2} \\ &= \frac{b-a}{2} \end{aligned} \qquad\qquad \begin{aligned} b - c_1 &= b - \frac{a+b}{2} \\ &= \frac{2b}{2} - \frac{a+b}{2} \\ &= \frac{b-a}{2} \end{aligned}$$

Since $b > a$, we see that $b - a > 0$ and so the previous equations show that $c_1 - a > 0$ and $b - c_1 > 0$. We can then conclude that $a < c_1 < b$.

We can now repeat this process by using $c_2 = \dfrac{c_1 + b}{2}$ and proving that $c_1 < c_2 < b$, In fact, for each natural number, we can define

$$c_{k+1} = \frac{c_k + b}{2}$$

and obtain the result that $a < c_1 < c_2 < \cdots < c_n < \cdots < b$ and this proves that the set $\{c_k \mid k \in \mathbb{N}$ is a countably infinite set where each element is a rational number between a and b. (A formal proof can be completed using mathematical induction. See Exercise ().

This result is true no matter how close together a and b are. For example, we can now conclude that there are infinitely many rational numbers between 0 and $\dfrac{1}{10000}$ This might suggest that the set $\mathbb{Q}$ of rational numbers is uncountable. Surprisingly, this is not the case. We start with a proof that the set of positive rational numbers is countable.

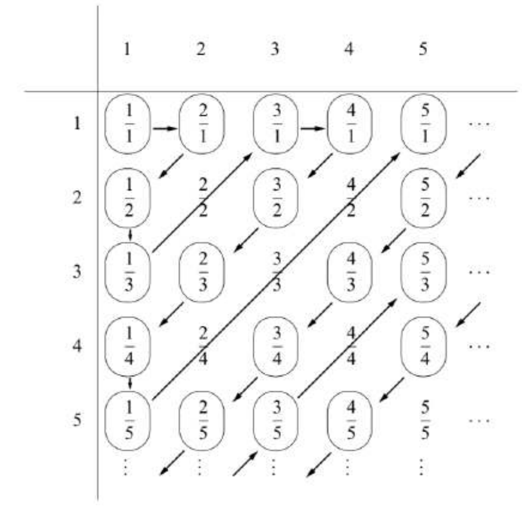
Theorem 9.14

The set of positive rational numbers is countably infinite.

Proof

We can write all the positive rational numbers in a two-dimensional array as shown in Figure 9.2. The top row in Figure 9.2 represents the numerator of the rational number, and the left column represents the denominator. We follow the arrows in Figure 9.2 to define $f : \mathbb{N} \to \mathbb{Q}^+$. The idea is to start in the upper left corner of the table and move to successive diagonals as follows:

- We start with all fractions in which the sum of the numerator and denominator is 2 (only $\frac{1}{1}$). So $f(1) = \frac{1}{1}$.



1 2 3 4 5
1 2 3 4 5
$\frac{1}{1}$ $\frac{2}{1}$ $\frac{3}{1}$ $\frac{4}{1}$ $\frac{5}{1}$ …
$\frac{1}{2}$ $\frac{2}{2}$ $\frac{3}{2}$ $\frac{4}{2}$ $\frac{5}{2}$ …
$\frac{1}{3}$ $\frac{2}{3}$ $\frac{3}{3}$ $\frac{4}{3}$ $\frac{5}{3}$ …
$\frac{1}{4}$ $\frac{2}{4}$ $\frac{3}{4}$ $\frac{4}{4}$ $\frac{5}{4}$ …
$\frac{1}{5}$ $\frac{2}{5}$ $\frac{3}{5}$ $\frac{4}{5}$ $\frac{5}{5}$ …
⋮ ⋮ ⋮ ⋮ ⋮

Figure 9.2: Counting the Positive Rational Numbers

- We next use those fractions in which the sum of the numerator and denominator is 3. So $f(2) = \frac{2}{1}$ and $f(3) = \frac{1}{2}$.

- We next use those fractions in which the sum of the numerator and denominator is 4. So $f(4) = \frac{1}{3}$, $f(5) = \frac{3}{1}$. We skipped $\frac{2}{2}$ since $\frac{2}{2} = \frac{1}{1}$. In this way, we will ensure that the function f is a one-to-one function.

We now continue with successive diagonals omitting fractions that are not in lowest terms. This process guarantees that the function f will be an injection and a surjection. Therefore, $\mathbb{N} \approx \mathbb{Q}^+$ and $\text{card}(\mathbb{Q}^+) = \aleph_0$.

Note: For another proof of Theorem 9.14, see exercise (14) on page 475.

Since $\mathbb{Q}^+$ is countable, it seems reasonable to expect that Q is countable. We will explore this soon. On the other hand, at this point, it may also seem reasonable to ask,

"Are there any uncountable sets?”

The answer to this question is yes, but we will wait until the next section to prove that certain sets are uncountable. We still have a few more issues to deal with concerning countable sets.

Countably Infinite Sets

Theorem 9.15.

If A is a countably infinite set, then $A \cup \{x\}$ is a countably infinite set.

Proof

Let A be a countably infinite set. Then there exists a bijection $f : \mathbb{N} \to A$. Since x is either in A or not in A, we can consider two cases.

If $x \in A$, then $A \cup \{x\} = A$ and $A \cup \{x\}$ is countably infinite.

If $x \notin A$, define $g : \mathbb{N} \to A \cup \{x\}$ by

$$g(n) = \begin{cases} x & \text{if } n = 1 \\ f(n-1) & \text{if } n > 1. \end{cases}$$

The proof that the function g is a bijection is Exercise (4). Since g is a bijection, we have proved that $A \cup \{x\} \approx \mathbb{N}$ and hence, $A \cup \{x\}$ is a countably infinite set.

Theorem 9.16.

If A is a countably infinite set and B is a finite set, then $A \cup B$ is a countably infinite set.

Proof

Exercise (5) on page 474.

Theorem 9.16 says that if we add a finite number of elements to a countably infinite set, the resulting set is still countably infinite. In other words, the cardinality of the new set is the same as the cardinality of the original set. Finite sets behave very differently in the sense that if we add elements to a finite set, we will change the cardinality. What may even be more surprising is the result in Theorem 9.17 that states that the union of two countably infinite (disjoint) sets is countably infinite. The proof of this result is similar to the proof that the integers are countably infinite (Theorem 9.13). In fact, if $A = \{a_1, a_2, a_3, ...\}$ and $B = \{b_1, b_2, b_3, ...\}$, then we can use the following diagram to help define a bijection from $\mathbb{N}$ to $A \cup B$.

Theorem 9.17

If A and B are disjoint countably infinite sets, then $A \cup B$ is a countably infinite set.

$$\begin{array}{ccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \cdots \\ a_1 & b_1 & a_2 & b_2 & a_3 & b_3 & a_4 & b_4 & a_5 & b_5 & \cdots \end{array}$$

Figure 9.3: A Function from $\mathbb{N}$ to $A \cup B$

Proof

Let A and B be countably infinite sets and let $f : \mathbb{N} \to A$ and $g : \mathbb{N} \to B$ be bijections. Define $h : \mathbb{N} \to A \cup B$ by

$$h(n) = \begin{cases} f(\dfrac{n+1}{2}) & \text{if } n \text{ is odd} \\ g(\dfrac{n}{2}) & \text{if } n \text{ is even.} \end{cases}$$

It is left as Exercise (6) on page 474 to prove that the function h is a bijection.

Since we can write the set of rational numbers Q as the union of the set of nonnegative rational numbers and the set of rational numbers, we can use the results in Theorem 9.14, Theorem 9.15, and Theorem 9.17 to prove the following theorem.

Theorem 9.18.

The set $\mathbb{Q}$ of all rational numbers is countably infinite.

Proof

Exercise (7) on page 474.

In Section 9.1, we proved that any subset of a finite set is finite (Theorem 9.6). A similar result should be expected for countable sets. We first prove that every subset of $\mathbb{N}$ is countable. For an infinite subset B of $\mathbb{N}$, the idea of the proof is to define a function $g : \mathbb{N} \to B$ by removing the elements from B from smallest to the next smallest to the next smallest, and so on. We do this by defining the function g recursively as follows:

- Let $g(1)$ be the smallest natural number in B.
- Remove $g(1)$ from B and let $g(2)$ be the smallest natural number in $B - \{g(1)\}$.
- Remove $g(2)$ and let $g(3)$ be the smallest natural number in $B - \{g(1), g(2)\}$.
- We continue this process. The formal recursive definition of $g : \mathbb{N} \to B$ is included in the proof of Theorem 9.19.

Theorem 9.19.

Every subset of the natural numbers is countable.

Proof

Let B be a subset of $\mathbb{N}$. If B is finte, then B is countable. So we next assume that B is infinite. We will next give a recursive definition of a function $g : \mathbb{N} \to B$ and then prove that g is a bijection.

- Let $g(1)$ be the smallest natural number in B.
- For each $n \in \mathbb{N}$, the set $B - \{g(1), g(2), ..., g(n)\}$ is not empty since B is infinte. Define $g(n+1)$ to be the smallest natural number in $B - \{g(1), g(2), ..., g(n)\}$.

The proof that the function g is a bijection is Exercise (11) on page 475.

Corollary 9.20.

Every subset of a countable set is countable.

Proof

Exercise (12) on page 475.

Exercise 9.2

1. State whether each of the following is true or false.

   (a) If a set A is countably infinite, then A is infinite.
   (b) If a set A is countably infinite, then A is countable.
   (c) If a set A is uncountable, then A is not countably infinite.
   (d) If $A \approx \mathbb{N}_k$ for some $k \in \mathbb{N}$, then A is not countable.
2. Prove that each of the following sets is countably infinite.

   (a) The set F^+ of all natural numbers that are multiple of 5
   (b) The set F of all integers that are multiples of 5
   (c) $\{\dfrac{1}{2^k} \mid k \in \mathbb{N}\}$
   (d) \{n \in \mathbb{Z}\ |\ n \ge -10\}\)
   (e) $\mathbb{N} - \{4, 5, 6\}$
   (f) \(\{m \in \mathbb{Z}\ |\ m \equiv 2\text{ (mod 3)\}\)
3. Prove part (2) of Theorem 9.10.
   Let A and B be sets. If A is infinite and $A \subseteq B$, then B is infinite.
4. Complete the proof of Theorem 9.15 by proving the following:
   Let A be a countably infinite set and $x \notin A$. If $f : \mathbb{N} \to A$ is a bijection, then g is a bijection, where $g : \mathbb{N} \to A \cup \{x\}$ by

$$g(n) = \begin{cases} x & \text{if } n = 1 \\ f(n-1) & \text{if } n > 1. \end{cases} \tag{9.2.7}$$

5. Prove Theorem 9.16.
   If A is a countably infinite set and B is a finite set, then $A \cup B$ is a countably infinite set.

   Hint: Let card(B) $= n$ and use a proof by induction on n. Theorem 9.15 is the basis step.

6. Complete the proof of Theorem 9.17 by proving the following:
   Let A and B be disjoint countably infinite sets and let $f : \mathbb{N} \to A$ and $g : \mathbb{N} \to B$ be bijections. Define $h : \mathbb{N} \to A \cup B$ by

$$h(n) = \begin{cases} f(\dfrac{n+1}{2} & \text{if } n \text{ is odd} \\ g(\dfrac{n}{2}) & \text{if } n \text{ is even.} \end{cases} \tag{9.2.8}$$

   Then the function h is a bijection.
7. Prove Theorem 9.18.
   The set $\mathbb{Q}$ of all rational numbers is countable.
   Hint: Use Theorem 9.15 and Theorem 9.17.
8. Prove that if A is countably infinite and B is finite, then $A - B$ is countably infinite.
9. Define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ as follows: For each $(m, n) \in \mathbb{N} \times \mathbb{N}$,

$$f(m, n) = 2^{m-1}(2n - 1). \tag{9.2.9}$$

   (a) Prove that f is an injection. **Hint:** If $f(m, n) = f(s, t)$, there are three cases to consider: $m > s$, $m < s$, and $m = s$. Use laws of exponents to prove that the first two cases lead to a contradiction.
   (b) Prove that f is a surjection. **Hint**: You may use the fact that if $y \in \mathbb{N}$, then $y = 2^k x$, where x is an odd natural number and k is a nonnegative integer. This is actually a consequence of the Fundamental Theorem of Arithmetic, Theorem 8.15. [See Exercise (13) in Section 8.2.]
   (c) Prove that $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$ and hence that card$(\mathbb{N} \times \mathbb{N}) = \aleph_0$.
10. Use Exercise (9) to prove that if A and B are countably infinite sets, then $A \times B$ is a countably infinite set.
11. Complete the proof of Theorem 9.19 by proving that the function g defined in the proof is a bijection from $\mathbb{N}$ to B.

Hint: To prove that g is an injection, it might be easier to prove that for all $r, s \in \mathbb{N}$, if $r \neq s$, then $g(r) \neq g(s)$. To do this, we may assume that $r < s$ since one of the two numbers must be less than the other. Then notice that $g(r) \in \{g(1), g(2), \ldots, g(s-1)\}$.

To prove that g is a surjection, let $b \in B$ and notice that for some $k \in \mathbb{N}$, there will be k natural numbers in B that are less than b.

12. Prove Corollary 9.20, which states that every subset of a countable set is countable.

    Hint: Let S be a countable set and assume that $A \subseteq S$. There are two cases: A is finite or A is infinite. If A is infinite, let $f : S \to \mathbb{N}$ be a bijection and define $g : A \to f(A)$ by $g(x) = f(x)$, for each $x \in A$.

13. Use Corollary 9.20 to prove that the set of all rational numbers between 0 and 1 is countably infinite.

Explorations and Activities

14. **Another Proof that $\mathbb{Q}^+$ Is Countable.** For this activity, it may be helpful to use the Fundamental Theorem of Arithmetic (see Theorem 8.15 on page 432). Let $\mathbb{Q}^+$ be the set of positive rational numbers. Every positive rational number has a unique representation as a fraction $\dfrac{m}{n}$, where m and n are relatively prime natural numbers. We will now define a function $f : \mathbb{Q}^+ \to \mathbb{N}$ as follows:

    If $x \in \mathbb{Q}^+$ and $x = \dfrac{m}{n}$, where $m, n \in \mathbb{N}$, $n \neq 1$ and $\gcd(m, n) = 1$, we write

$$\begin{aligned} m &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \text{ and} \\ n &= q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}, \end{aligned} \tag{9.2.10}$$

where $p_1, p_2, \ldots, p_r$ are distinct prime numbers, $q_1, q_2, \ldots, q_s$ are distinct prime numbers, and $\alpha_1, \alpha_2, \ldots, \alpha_r$ and $\beta_1, \beta_2, \ldots, \beta_s$ are natural numbers.
We also write $1 = 2^0$ when $m = 1$. We then define

$$f(x) = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_r^{2\alpha_r} q_1^{2\beta_1 - 1} q_2^{2\beta_2 - 1} \cdots q_s^{2\beta_s - 1}. \tag{9.2.11}$$

If $x = \dfrac{m}{1}$, then we define $f(x) = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_r^{2\alpha_r} = m^2$.

(a) Determine $f(\frac{2}{3})$, $f(\frac{5}{6})$, $f(6)$, $f(\frac{12}{25})$, $f(\frac{375}{392})$, and $f(\frac{2^3 \cdot 11^3}{3 \cdot 5^4})$.
(b) If possible, find $x \in \mathbb{Q}^+$ such that $f(x) = 100$.
(c) If possible, find $x \in \mathbb{Q}^+$ such that $f(x) = 12$.
(d) If possible, find $x \in \mathbb{Q}^+$ such that $f(x) = 2^8 \cdot 3^5 \cdot 13 \cdot 17^2$.
(e) Prove that the function f is an injection.
(f) Prove that the function f is a surjection.
(g) What has been proved?

Answer

Add texts here. Do not delete this text first.

This page titled 9.2: Countable Sets is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

9.3: Uncountable Sets

? Preview Activity 9.3.1: The Game of Dodge Ball

(From The Heart of Mathematics: *An Invitation to Effective Thinking* by Edward B. Burger and Michael Starbird, Key Publishing Company, ©2000 by Edward B. Burger and Michael Starbird.)

Dodge Ball is a game for two players. It is played on a game board such as the one shown in Figure 9.4. Player One has a 6 by 6 array to complete and Player Two has a 1 by 6 row to complete. Each player has six turns as described next.

- Player One begins by filling in the first horizontal row of his or her table with a sequence of six X's and O's, one in each square in the first row.
- Then Player Two places either an X or an O in the first box of his or her row. At this point, Player One has completed the first row and Player Two has filled in the first box of his or her row with one letter.

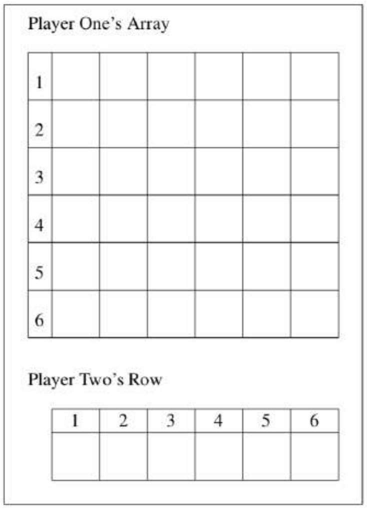


Figure 9.4: Game Board for Dodge Ball

- The game continues with Player One completing a row with six letters (X's and O's), one in each box of the next row followed by Player Two writing one letter (an X or an O) in the next box of his or her row. The game is completed when Player One has completed all six rows and Player Two has completed all six boxes in his or her row.

Winning the Game

- Player One wins if any horizontal row in the 6 by 6 array is identical to the row that Player Two created. (Player One matches Player Two.)
- Player Two wins if Player Two's row of six letters is different than each of the six rows produced by Player One. (Player Two "dodges" Player One.)

There is a winning strategy for one of the two players. This means that there is plan by which one of the two players will always win. Which player has a winning strategy? Carefully describe this winning strategy.

Applying the Winning Strategy to Lists of Real Numbers

Following is a list of real numbers between 0 and 1. Each real number is written as a decimal number.

$$\begin{aligned} a_1 &= 0.1234567890 & a_6 &= 0.0103492222 \\ a_2 &= 0.3216400000 & a_7 &= 0.0011223344 \\ a_3 &= 0.4321593333 & a_8 &= 0.7077700022 \\ a_4 &= 0.9120930092 & a_9 &= 0.2100000000 \\ a_5 &= 0.0000234102 & a_{10} &= 0.9870008943 \end{aligned}$$

Use a method similar to the winning strategy in Cantor's dodge ball to write a real number (in decimal form) between 0 and 1 that is not in this list of 10 numbers.

1. Do you think your method could be used for any list of 10 real numbers between 0 and 1 if the goal is to write a real number between 0 and 1 that is not in the list?
2. Do you think this method could be extended to a list of 20 different real numbers? To a list of 50 different real numbers?
3. Do you think this method could be extended to a list consisting of countably infinite list of real numbers?

? Preview Activity 9.3.2: Functions from a Set to Its Power Set

Let A be a set. In Section 5.1, we defined the power set $\mathcal{P}(A)$ of A to be the set of all subsets of A. This means that

$$X \in \mathcal{P}(A) \text{ if and only if } X \subseteq A.$$

Theorem 5.5 in Section 5.1 states that if a set A has n elements, then A has 2^n subsets or that $\mathcal{P}(A)$ has 2^n elements. Using our current notation for cardinality, this means that

if $\text{card}(A) = n$, then $\text{card}(\mathcal{P}(A) = 2^n$.

(The proof of this theorem was Exercise (17) on page 229.)

We are now going to define and explore some functions from a set A to its power set $\mathcal{P}(A)$. This means that the input of the function will be an element of A and the output of the function will be a subset of A.

1. Let $A = \{1, 2, 3, 4\}$. Define $f : A \to \mathcal{P}(A)$ by
   $f(1) = \{1, 2, 3\}$ $f(3) = \{1, 4\}$
   $f(2) = \{1, 3, 4\}$ $f(4) = \{2, 4\}$.

   (a) Is $1 \in f(1)$? Is $2 \in f(2)$? Is $3 \in f(3)$? Is $4 \in f(4)$?
   (b) Determine $S = \{x \in A \mid x \notin f(x)\}$.
   (c) Notice that $S \in \mathcal{P}(A)$. Does there exist an element t in A such that $f(t) = S$? That is, is $S \in \text{range}(f)$?
2. Let $A = \{1, 2, 3, 4\}$. Define $f : A \to \mathcal{P}(A)$ by

   $$f(x) = A - \{x\} \text{ for each } x \in A. \tag{9.3.1}$$

   (a) Determine $f(1)$. Is $1 \in f(1)$?
   (b) Determine $f(2)$. Is $2 \in f(2)$?
   (c) Determine $f(3)$. Is $3 \in f(3)$?
   (d) Determine $f(4)$. Is $4 \in f(4)$?
   (e) Determine $S = \{x \in A \mid x \notin f(x)\}$.
   (f) Notice that $S \in \mathcal{P}(A)$. Does there exist an element t in A such that $f(t) = S$? That is, is $S \in \text{range}(f)$?
3. Define $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ by

   $$f(n) - \mathbb{N} - \{n^2, n^2 - 2n\}, \text{ for each} n \in \mathbb{N}. \tag{9.3.2}$$

   (a) Determine $f(1)$, $f(2)$, $f(3)$, and $f(4)$. In each of these cases, determine if $k \in f(k)$.
   (b) Prove that if $n > 3$, then $n \in f(n)$. **Hint**: Prove that if $n > 3$, then $n^2 > n$ and $n^2 - 2n > n$.
   (c) Determine $S = \{x \in \mathbb{N} \mid x \notin f(x)\}$.
   (d) Notice that $S \in \mathcal{P}(\mathbb{N})$. Does there exist an element t in $\mathbb{N}$ such that $f(t) = S$? That is, is $S \in \text{range}(f)$?

We have seen examples of sets that are countably infinite, but we have not yet seen an example of an infinite set that is uncountable. We will do so in this section. The first example of an uncountable set will be the open interval of real numbers (0, 1). The proof that this interval is uncountable uses a method similar to the winning strategy for Player Two in the game of Dodge Ball from Preview Activity 1. Before considering the proof, we need to state an important results about decimal expressions for real numbers.

Decimal Expressions for Real Numbers

In its decimal form, any real number a in the interval (0, 1) can be written as $a = 0.a_1a_2a_3a_4...$, where each a_i is an integer with $0 \le a_i \le 9$. For example,

$$\frac{5}{12} = 0.416666...$$

We often abbreviate this as $\frac{5}{12} = 0.41\overline{6}$ to indicate that the 6 is repeated. We can also repeat a block of digits. For example, $\frac{5}{26} = 0.19\overline{230769}$ to indicate that the block 230769 repeats. That is

$$\frac{5}{26} = 0.19230769230769230769...$$

There is only one situation in which a real number can be represented as a decimal in more than one way. A decimal that ends with an infinite string of 9's is equal to one that ends with an infinite string of 0's. For example, 0.3199999... . represents the same real number as 0.3200000... . Geometric series can be used to prove that a decimal that ends with an infinite string of 9's is equal to one that ends with an infinite string of 0's, but we will not do so here.

Definition

A decimal representation of a real number a is in **normalized form** provided that there is no natural number k such that for all natural numbers n with $n > k$, $a_n = 9$. That is, the decimal representation of a is in normalized form if and only if it does not end with an infinite string of 9's.

One reason the normalized form is important is the following theorem (which will not be proved here).

Theorem 9.21

Two decimal numbers in normalized form are equal if and only if they have identical digits in each decimal position.

Uncountable Subsets of $\mathbb{R}$

In the proof that follows, we will use only the normalized form for the decimal representation of a real number in the interval (0, 1).

Theorem 9.22.

The open interval (0, 1) is an uncountable set.

Proof

Since the interval (0, 1) contains the infinite subset�� $\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, ...\}$, we can use Theorem 9.10, to conclude that (0, 1) is an infinite set. So (0, 1) is either countably infinite or uncountable. We will prove that (0, 1) is uncountable by proving that any injection from (0, 1) to $\mathbb{N}$ cannot be a surjection, and hence, there is no bijection between (0, 1) and $\mathbb{N}$.

So suppose that the function $f : \mathbb{N} \to (0, 1)$ is an injection. We will show that f cannot be a surjection by showing that there exists an element in (0, 1) that cannot be in the range of f. Writing the images of the elements of $\mathbb{N}$ in normalized form, we can write

$$\begin{aligned}
f(1) &= 0.a_{11}a_{12}a_{13}a_{14}a_{15}... \\
f(2) &= 0.a_{21}a_{22}a_{23}a_{24}a_{25}... \\
f(3) &= 0.a_{31}a_{32}a_{33}a_{34}a_{35}... \\
f(4) &= 0.a_{41}a_{42}a_{43}a_{44}a_{45}... \\
f(5) &= 0.a_{51}a_{52}a_{53}a_{54}a_{55}... \\
&... \\
f(n) &= 0.a_{n1}a_{n2}a_{n3}a_{n4}a_{n5}... \\
&...
\end{aligned}$$

Notice the use of the double subscripts. The number a_{ij} is the jth digit to the right of the decimal point in the normalized decimal representation of $f(i)$.

We will now construct a real number $b = 0.b_1b_2b_3b_4b_5...$ in (0, 1) and in normalized form that is not in this list.

Note: The idea is to start in the upper left corner and move down the diagonal in a manner similar to the winning strategy for Player Two in the game in Preview Activity 1. At each step, we choose a digit that is not equal to the diagonal digit.

Start with a_{11} in $f(1)$. We want to choose b_1 so that $b_1 \neq 0$, $b_1 \neq a_{11}$, and $b_1 \neq 9$. (To ensure that we end up with a decimal that is in normalized form, we make sure that each digit is not equal to 9.) We then repeat this process with a_{22}, a_{33}, a_{44}, a_{55}, and so on. So we let b be the real number $b = 0.b_1b_2b_3b_4b_5\ldots$, where for each $k \in \mathbb{N}$

$$b_k = \begin{cases} 3 & \text{if } a_{kk} \neq 3 \\ 5 & \text{if } a_{kk} = 3. \end{cases}$$

(The choice of 3 and 5 is arbitrary. Other choices of distinct digits will also work.)

Now for each $n \in \mathbb{N}$, $b \neq f(n)$ since b and $f(n)$ are in normalized form and b and $f(n)$ differ in the nth decimal place. This proves that any function from $\mathbb{N}$ to (0, 1) cannot be surjection and hence, there is no bijection from $\mathbb{N}$ to (0, 1). Therefore, (0, 1) is not countably infinite and hence must be an uncountable set.

? Progress Check 9.23 (Dodge Ball and Cantor's Diagonal Argument)

The proof of Theorem 9.22 is often referred to as **Cantor's diagonal argument**. It is named after the mathematician Georg Cantor, who first published the proof in 1874. Explain the connection between the winning strategy for Player Two in Dodge Ball (see Preview Activity 1) and the proof of Theorem 9.22 using Cantor's diagonal argument.

Answer

Add texts here. Do not delete this text first.

The open interval (0, 1) is our first example of an uncountable set. The cardinal number of (0, 1) is defined to be c, which stands for **the cardinal number of the continuum**. So the two infinite cardinal numbers we have seen are $\aleph_0$ for countably infinite sets and c.

Definition

A set A is said to have **cardinality** c provided that A is equivalent to (0, 1). In this case, we write $\text{card}(A) = c$ and say that the cardinal number of A is c.

The proof of Theorem 9.24 is included in Progress Check 9.25.

Theorem 9.24.

Let a and b be real numbers with $a < b$. The open interval (a, b) is uncountable and has cardinality c.

Proof

Add proof here and it will automatically be hidden

? Progress Check 9.25 (Proof of Theorem 9.24)

1. In Part (3) of Progress Check 9.2, we proved that if $b \in \mathbb{R}$ and $b > 0$, then the open interval (0, 1) is equivalent to the open interval (0, b). Now let a and b be real numbers with $a < b$. Find a function

$$f : (0, 1) \to (a, b) \tag{9.3.3}$$

   that is a bijection and conclude that $(0, 1) \approx (a, b)$.
   Hint: Find a linear function that passes through the points (0, a) and (1, b). Use this to define the function f. Make sure you prove that this function f is a bijection.
2. Let a, b, c, d be real numbers with $a < b$ and $c < d$. Prove that $(a, b) \approx (c, d)$.

Answer

Add texts here. Do not delete this text first.

Theorem 9.26.

The set of real numbers $\mathbb{R}$ is uncountable and has cardinality c.

Proof

Let $f:(-\frac{\pi}{2},\frac{\pi}{2})\to\mathbb{R}$ be defined by $f(x)=tan x$, for each $x\in\mathbb{R}$. The function f is as bijection and, hence, $(-\frac{\pi}{2},\frac{\pi}{2})\approx\mathbb{R}$. So by Theorem 9.24, $\mathbb{R}$ is uncountable and has cardinality c.

Cantor's Theorem

We have now seen two different infinite cardinal numbers, $\aleph_0$ and c. It can seem surprising that there is more than one infinite cardinal number. A reasonable question at this point is, "Are there any other infinite cardinal numbers?" The astonishing answer is that there are, and in fact, there are infinitely many different infinite cardinal numbers. The basis for this fact is the following theorem, which states that a set is not equivalent to its power set. The proof is due to Georg Cantor (1845–1918), and the idea for this proof was explored in Preview Activity 2. The basic idea of the proof is to prove that any function from a set A to its power set cannot be a surjection.

Theorem 9.27 (Cantor's Theorem).

For every set A, A and $\mathcal{P}(A)$ do not have the same cardinality.

Proof

Let A be a set. If $A=\emptyset$, then $\mathcal{P}(A)=\{\emptyset\}$, which has cardinality 1. Therefore, $\emptyset$ and $\mathcal{P}(\emptyset)$ do not have the same cardinality.

Now suppose that $A\neq\emptyset$, and let $f:A\to\mathcal{P}(A)$. We will show that f cannot be a surjection, and hence there is no bijection from A to $\mathcal{P}(A)$. This will prove that A is not equivalentt to $\mathcal{P}(A)$. Define

$$S=\{x\in A\mid x\notin f(x)\}.$$

Assume that there exists a t in A such that $f(t)=S$. Now, either $f\in S$ to $t\notin S$.

- If $t\in S$, then $t\in\{x\in A\mid x\notin f(x)\}$. By the definition of S, this means that $t\notin f(t)$. However, $f(t)=S$ and so we conclude that $t\notin S$. But now we have $t\in S$ and $t\notin S$. This is a contradiction.
- If $t\notin S$, then $t\notin\{x\in A\mid x\notin f(x)\}$. By the definition of S, this means that $t\in f(t)$. However, $f(t)=S$ and so we conclude that $t\in S$. But now we have $t\notin S$ and $t\in S$. This is a contradiction.

So in both cases we have arrived at a contradiction. This means that there does not exist a t in A such that $f(t)=S$. Therefore, any function from A to $\mathcal{P}(A)$ is not a surjection and hence not a bijection. Hence, A and $\mathcal{P}(A)$ do not have the same cardinality.

corollary 9.28.

$\mathcal{P}(\mathbb{N})$ is an infinite set that is not countably infinite.

Proof

Since $\mathcal{P}(\mathbb{N})$ contains the infinite subset $\{\{1\},\{2\},\{3\}...\}$, we can use Theorem 9.10, to conclude that $\mathcal{P}(\mathbb{N})$ is an infinite set. By Cantor's Theorem (Theorem 9.27), $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$ do not have the same cardinality. Therefore, P.N/ is not countable and hence is an uncountable set.

Some Final Comments about Uncountable Sets

1. We have now seen that any open interval of real numbers is uncountable and has cardinality c. In addition, R is uncountable and has cardinality c. Now, Corollary 9.28 tells us that P.N/ is uncountable. A question that can be asked is,

$$\text{"Does } \mathcal{P}(\mathbb{N}) \text{ have the same cardinality as } \mathbb{R}\text{?"} \tag{9.3.4}$$

The answer is yes, although we are not in a position to prove it yet. A proof of this fact uses the following theorem, which is known as the Cantor-Schrӧder-Bernstein Theorem.

Theorem 9.29. Cantor-Schrӧder-Bernstein

Let A and B be sets. If there exist injections $f : A \to B$ and $g : B \to A$, then $A \approx B$

In the statement of this theorem, notice that it is not required that the function g be the inverse of the function f. We will not prove the Cantor-Schrӧder-Bernstein Theorem here. The following items will show some uses of this important theorem.

2. The Cantor-Schrӧder-Bernstein Theorem can also be used to prove that the closed interval [0, 1] is equivalent to the open interval (0, 1). See Exercise (6) on page 486.
3. Another question that was posed earlier is,

$$\text{"Are there other infinite cardinal numbers other than } \aleph_0 \text{ and } c\text{?"} \tag{9.3.5}$$

Again, the answer is yes, and the basis for this is Cantor's Theorem (Theorem 9.27). We can start with $\text{card}(\mathbb{N}) = \aleph_0$. We then define the following infinite cardinal numbers:

$$\begin{array}{ll} \text{card}(\mathcal{P}(\mathbb{N})) = \alpha_1. & \text{card}(\mathcal{P}(((\mathbb{N})))) = \alpha_1. \\ \text{card}(\mathcal{P}((\mathbb{N}))) = \alpha_1. & \dots \end{array} \tag{9.3.6}$$

Cantor's Theorem tells us that these are all different cardinal numbers, and so we are just using the lowercase Greek letter α (alpha) to help give names to these cardinal numbers. In fact, although we will not define it here, there is a way to "order" these cardinal numbers in such a way that

$$\aleph_0 < \alpha_1 < \alpha_2 < \alpha_3 < \cdots. \tag{9.3.7}$$

Keep in mind, however, that even though these are different cardinal numbers, Cantor's Theorem does not tell us that these are the only cardinal numbers.

4. In Comment (1), we indicated that $\mathcal{P}(\mathbb{N})$ and $\mathbb{R}$ have the same cardinality. Combining this with the notation in Comment (3), this means that

$$\alpha_1 = c. \tag{9.3.8}$$

However, this does not necessarily mean that c is the "next largest" cardinal number after $\aleph_0$. A reasonable question is, "Is there an infinite set with cardinality between $\aleph_0$ and c?" Rewording this in terms of the real number line, the question is, "On the real number line, is there an infinite set of points that is not equivalent to the entire line and also not equivalent to the set of natural numbers?" This question was asked by Cantor, but he was unable to find any such set. He conjectured that no such set exists. That is, he conjectured that c is really the next cardinal number after $\aleph_0$. This conjecture has come to be known as the **Continuum Hypothesis**. Stated somewhat more formally, the Continuum Hypothesis is

$$\text{There is no set } X \text{ such that } \aleph_0 < \text{card}(X) < c. \tag{9.3.9}$$

The question of whether the Continuum Hypothesis is true or false is one of the most famous problems in modern mathematics.

Through the combined work of Kurt Gӧdel in the 1930s and Paul Cohen in 1963, it has been proved that the Continuum Hypothesis cannot be proved or disproved from the standard axioms of set theory. This means that either the Continuum Hypothesis or its negation can be added to the standard axioms of set theory without creating a contradiction.

Exercise 9.3

1. Use an appropriate bijection to prove that each of the following sets has cardinality c.

   (a) $(0, \infty)$
   (b) (a, ∞), for any $a \in \mathbb{R}$

(c) $\mathbb{R} - \{0\}$
(d) $\mathbb{R} - \{a\}$, for any $a \in \mathbb{R}$

2. Is the set of irrational numbers countable or uncountable? Prove that your answer is correct.
3. Prove that if A is uncountable and $A \subseteq B$, then B is uncountable.
4. Do two uncountable sets always have the same cardinality? Justify your conclusion.
5. Let C be the set of all infinite sequences, each of whose entries is the digit 0 or the digit 1. For example,

$$\begin{aligned}(1,0,1,0,1,0,1,0,\ldots) &\in C;\\(0,1,0,1,1,0,1,1,1,0,1,1,1,1,\ldots) &\in C;\\(2,1,0,1,1,0,1,1,1,0,1,1,1,1,\ldots) &\notin C.\end{aligned} \tag{9.3.10}$$

   Is the set C a countable set or an uncountable set? Justify your conclusion.
6. The goal of this exercise is to use the Cantor-Schr$\ddot{o}$der-Bernstein Theorem to prove that the cardinality of the closed interval [0, 1]�� is c.

   (a) Find an injection $f : (0,1) \to [0,1]$.
   (b) Find an injection $h : [0,1] \to (-1,2)$.
   (c) Use the fact that $(-1,2) \approx (0,1)$ to prove that there exists an injection $g : [0,1] \to (0,1)$. (It is only necessary to prove that the injection g exists. It is not necessary to determine a specific formula for $g(x)$.)
   Note: Instead of doing Part (b) as stated, another approach is to find an injection $k : [0,1] \to (0,1)$. Then, it is possible to skip Part (c) and go directly to Part (d).
   (d) Use the Cantor-Schr$\ddot{o}$der-Bernstein Theorem to conclude that $[0,1] \approx (0,1)$ and hence that the cardinality of [0, 1] is c.
7. In Exercise (6), we proved that the closed interval [0, 1] is uncountable and has cardinality c. Now let $a, b \in \mathbb{R}$ with $a < b$. Prove that $[a,b] \approx [0,1]$ and hence that $[a,b]$ is counttable and has cardinality c.
8. Is the set of all finite subsets of $\mathbb{N}$ countable or uncountable? Let F be the set of all finite subsets of $\mathbb{N}$. Determine the cardinality of the set F.

   Consider defining a function $f : F \to \mathbb{N}$ that produces the following.
   - If $A = \{1,2,6\}$, then $f(A) = 2^1 3^2 5^6$.
   - If $B = \{3,6\}$, then $f(B) = 2^3 3^6$.
   - If $C = \{m_1, m_2, m_3, m_4\}$ with $m_1 < m_2 < m_3 < m_4$, then $f(C) = 2^{m_1} 3^{m_2} 5^{m_3} 7^{m_4}$.

   It might be helpful to use the Fundamental Theorem of Arithmetic on page 432and to denote the set of all primes as $P = \{p_1, p_2, p_3, p_4, \ldots\}$ with $p_1 > p_2 < p_3 < p_4 \cdots$. Using the sets A, B, and C define above, we could then write $f(A) = p_1^1 p_2^2 p_3^6$, $f(B) = p_1^3 p_2^6$, and $f(C) = p_1^{m_1} p_2^{m_2} p_3^{m_3} p_4^{m_4}$.
9. In Exercise (2), we showed that the set of irrational numbers is uncountable. However, we still do not know the cardinality of the set of irrational numbers. Notice that we can use $\mathbb{Q}^c$ to stand for the set of irrational numbers.

   (a) Construct a function $f : \mathbb{Q}^c \to \mathbb{R}$ that is an injection.

   We know that any real number a can be represented in decimal form as follows:

$$a = A.a_1 a_2 a_3 a_4 \cdots a_n \cdots, \tag{9.3.11}$$

   where A is an integer and the decimal part ($0.a_1 a_2 a_3 a_4 \cdots$) is in normalized form. (See page 480.) We also know that the real number a is an irrational number if and only a has an infinite non-repeating decimal expansion. We now associate with a the real number

$$A.a_1 0 a_2 11 a_3 000 a_4 1111 a_5 00000 a_6 111111 \cdots. \tag{9.3.12}$$

   Notice that to construct the real number in (9.3.12), we started with the decimal expansion of a, inserted a 0 to the right of the first digit after the decimal point, inserted two 1's to the right of the second digit to the right of the decimal point, inserted three 0's to the right of the third digit to the right of the decimal point, and so on.

(b) Explain why the real number in (9.3.12) is an irrational number.
(c) Use these ideas to construct a function $g:\mathbb{R}\to\mathbb{Q}^c$ that is an injection.
(d) What can we now conclude by using the Cantor-Schröder-Bernstein Theorem?

10. Let J be the unit open interval. That is, $J=\{x\in\mathbb{R}\mid 0<x<1\}$ and let $S=\{(x,y)\in\mathbb{R}\times\mathbb{R}\mid 0<x<1 \text{ and } 0<y<1\}$. We call S the unit open square. We will now define a function f from S to J. Let $(a,b)\in S$ and write the decimal expansions of a and b in normalized form as

$$\begin{aligned} a &= 0.a_1a_2a_3a_4\cdots a_n\cdots \\ b &= 0.b_1b_2b_3b_4\cdots b_n\cdots. \end{aligned} \tag{9.3.13}$$

We then define $f(a,b)=0.a_1b_1a_2b_2a_3b_3a_4b_4\cdots a_nb_n\cdots$.

(a) Determine the values of $f(0.3,0.625)$, $f(\frac{1}{3},\frac{1}{4})$, and $f(\frac{1}{6},\frac{5}{6})$.
(b) If possible, find $(x,y)\in S$ such that $f(x,y)=0.2345$.
(c) If possible, find $(x,y)\in S$ such that $f(x,y)=\frac{1}{3}$.
(d) If possible, find $(x,y)\in S$ such that $f(x,y)=\frac{1}{2}$.
(e) Explain why the function $f:S\to J$ is an injection but is not a surjection.
(f) Use the Cantor-Schröder-Bernstein Theorem to prove that the cardinality of the unit open square S is equal to c. If this result seems surprising, you are in good company. In a letter written in 1877 to the mathematician Richard Dedekind describing this result that he had discovered, Georg Cantor wrote, "I see it but I do not believe it."

Explorations and Activities

11. **The Closed Interval [0,1].** In Exercise (6), the Cantor-Schröder-Bernstein Theorem was used to prove that the closed interval [0, 1] has cardinality c. This may seem a bit unsatisfactory since we have not proved the Cantor-Schröder-Bernstein Theorem. In this activity, we will prove that card$([0,1])=c$ by using appropriate bijections.

(a) Let $f:[0,1]\to[0,1)$ by

$$f(x)=\begin{cases} \frac{1}{2} & \text{if } x=0 \\ \frac{1}{n+1} & \text{if } x=\frac{1}{2} \text{ for some } n\in\mathbb{N} \\ x & \text{otherwise.} \end{cases} \tag{9.3.14}$$

i. Determine $f(0)$, $f(1)$, $f(\frac{1}{2})$, $f(\frac{1}{3})$, $f(\frac{1}{4})$, and $f(\frac{1}{5})$.
ii. Sketch a graph of the function f. **Hint**: Start with the graph of $y=x$ for $0\le x\le 1$. Remove the point (1, 1) and replace it with the point (1, $\frac{1}{2}$). Next, remove the point $(\frac{1}{2},\frac{1}{2})$ and replace it with the point $(\frac{1}{2},\frac{1}{3})$. Continue this process of removing points on the graph of $y=x$ and replacing them with the points determined from the information in Part (11(a)i). Stop after repeating this four or five times so that pattern of this process becomes apparent.
iii. Explain why the function f is a bijection.
iv. Prove that $[0,1]\approx[0,1)$.

(b) Let $g:[0,1)\to(0,1)$ by

$$g(x)=\begin{cases} \frac{1}{n+1} & \text{if } x=\frac{1}{2} \text{ for some } n\in\mathbb{N} \\ x & \text{otherwise.} \end{cases} \tag{9.3.15}$$

i. Follow the procedure suggested in Part (11a) to sketch a graph of g.
ii. Explain why the function g is a bijection.
iii. Prove that $[0,1)\approx(0,1)$.
(c) Prove that [0, 1] and [0, 1) are both uncountable and have cardinality c.

Answer

Add texts here. Do not delete this text first.

This page titled 9.3: Uncountable Sets is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

9.S: Finite and Infinite Sets (Summary)

Important Definitions

- Equivalent sets, page 452
- Sets with the same cardinality, page 452
- Finite set, page 455
- Infinite set, page 455
- Cardinality of a finite set, page 455
- Cardinality of $\mathbb{N}$, page 466
- $\aleph_0$, page 466
- Countably infinite set, page 466
- Denumerable set, page 466
- Uncountable set, page 466

Important Theorems and Results about Finite and Infinite Sets

- **Theorem 9.3.** Any set equivalent to a finite nonempty set A is a finite set and has the same cardinality as A.
- **Theorem 9.6**. If S is a finite set and A is a subset of S, then A is finite and $\text{card}(A) \le \text{card}(S)$.
- **Corollary 9.8**. A finite set is not equivalent to any of its proper subsets.
- **Theorem 9.9 [The Pigeonhole Principle]**. Let A and B be finite sets. If $\text{card}(A) > \text{card}(B)$, then any function $f : A \to B$ is not an injection.
- **Theorem 9.10**. Let A and B be sets.

  1. If A is infinite and $A \approx B$, then B is infinite.
  2. If A is infinite and $A \subseteq B$,then B is infinite.
- **Theorem 9.13**. The set $\mathbb{Z}$ of integers is countably infinite, and so card$(\mathbb{Z}) = \aleph_0$.
- **Theorem 9.14**. The set of positive rational numbers is countably infinite.
- **Theorem 9.16**. If A is a countably infinite set and B is a finite set, then $A \cup B$ is a countably infinite set.
- **Theorem 9.17**. If A and B are disjoint countably infinite sets, then $A \cup B$ is a countably infinite set.
- **Theorem 9.18**. The set $\mathbb{Q}$ of all rational numbers is countably infinite.
- **Theorem 9.19**. Every subset of the natural numbers is countable.
- **Corollary 9.20**. Every subset of a countable set is countable.
- **Theorem 9.22**. The open interval (0, 1) is an uncountable set.
- **Theorem 9.24**. Let a and b be real numbers with $a < b$. The open interval (a, b) is uncountable and has cardinality c.
- **Theorem 9.26.** The set of real numbers $\mathbb{R}$ is uncountable and has cardinality c.
- **Theorem 9.27 [Cantor's Theorem]**. For every set A, A and $\mathcal{P}(A)$ do not have the same cardinality.
- **Corollary 9.28.** $\mathcal{P}(\mathbb{N})$ is an infinite set that is not countably infinite.
- **Theorem 9.29 [Cantor-Schr$\ddot{0}$der-Bernstein]**. Let A and B be sets. If there exist injections $f_1 : A \to B$ and $f_2 : B \to A$, then $A \approx B$.

This page titled 9.S: Finite and Infinite Sets (Summary) is shared under a CC BY-NC-SA 3.0 license and was authored, remixed, and/or curated by Ted Sundstrom (ScholarWorks @Grand Valley State University) via source content that was edited to the style and standards of the LibreTexts platform.

Index

A
absolute value
3.4: Using Cases in Proofs

B
Biconditional Statement
2.1: Statements and Logical Operators
bijection
6.3: Injections, Surjections, and Bijections

C
Cantor’s theorem
9.3: Uncountable Sets
cardinality
5.1: Sets and Operations on Sets
9.1: Finite Sets
Cartesian plane
5.4: Cartesian Products
Cartesian Products
5.4: Cartesian Products
cases
3.4: Using Cases in Proofs
closure
1.1: Statements and Conditional Statements
codomain
6.1: Introduction to Functions
common divisor
8.1: The Greatest Common Divisor
composite function
6.4: Composition of Functions
composite number
8.2: Prime Numbers and Prime Factorizations
composition of functions
6.4: Composition of Functions
compound statements
2.1: Statements and Logical Operators
conditional statement
1.1: Statements and Conditional Statements
congruence
3.1: Direct Proofs
3.5: The Division Algorithm and Congruence
Congruence Classes
7.3: Equivalence Classes
7.4: Modular Arithmetic
congruence modulo n
7.2: Equivalence Relations
convex polygons
6.2: More about Functions
countable sets
9.2: Countable Sets

D
De Morgan's Laws
2.2: Logically Equivalent Statements
5.3: Properties of Set Operations
5.5: Indexed Families of Sets
Decomposing Functions
6.4: Composition of Functions
definition by recursion
4.3: Induction and Recursion
denumerable set
9.2: Countable Sets
diagonal
6.2: More about Functions
Diophantine Equations
8.3: Linear Diophantine Equations
Direct Proofs
3.1: Direct Proofs
disjoint sets
5.2: Proving Set Relationships
Division Algorithm
3.5: The Division Algorithm and Congruence

E
equivalence classes
7.3: Equivalence Classes
equivalence relations
7: Equivalence Relations
7.2: Equivalence Relations
Euclid’s Lemma
8.2: Prime Numbers and Prime Factorizations
Euclidean Algorithm
8.1: The Greatest Common Divisor

F
factorial
4.2: Other Forms of Mathematical Induction
Fibonacci Numbers
4.3: Induction and Recursion
Finite Sets
9.1: Finite Sets
function
6.1: Introduction to Functions

G
Geometric Sequences
4.3: Induction and Recursion
geometric series
4.3: Induction and Recursion
greatest common divisor
8.1: The Greatest Common Divisor

I
indexing set
5.5: Indexed Families of Sets
induction
4.1: The Principle of Mathematical Induction
inductive assumption
4.1: The Principle of Mathematical Induction
inductive hypothesis
4.1: The Principle of Mathematical Induction
injection
6.3: Injections, Surjections, and Bijections
intersection
5.1: Sets and Operations on Sets
inverse function
6.5: Inverse Functions

L
LOGICAL EQUIVALENCY
3.4: Using Cases in Proofs

M
modular arithmetic
7.4: Modular Arithmetic

N
number theory
8: Topics in Number Theory

O
Open Sentences
2.3: Open Sentences and Sets
ordered pairs
6.5: Inverse Functions

P
perfect square
2.4: Quantifiers and Negations
Pigeonhole Principle
9.1: Finite Sets
polygon
6.2: More about Functions
power set
5.1: Sets and Operations on Sets
Prime Factorizations
8.2: Prime Numbers and Prime Factorizations
prime numbers
8.2: Prime Numbers and Prime Factorizations
proper subset
5.1: Sets and Operations on Sets
proposition
1.1: Statements and Conditional Statements
propositional function
2.3: Open Sentences and Sets

R
range
6.1: Introduction to Functions
recursion
4.3: Induction and Recursion
regular polygon
6.2: More about Functions
relations
7.1: Relations
Relatively Prime Integers
8.2: Prime Numbers and Prime Factorizations
roster method
2.3: Open Sentences and Sets

S
sequence
4.3: Induction and Recursion
6.2: More about Functions
sequences
6.2: More about Functions
set notation
2.3: Open Sentences and Sets
set operations
5.1: Sets and Operations on Sets
set theory
5: Set Theory

sets
  2.3: Open Sentences and Sets
  5.1: Sets and Operations on Sets
surjection
  6.3: Injections, Surjections, and Bijections

T
triangle inequality
  3.4: Using Cases in Proofs
Truth Table
  2.1: Statements and Logical Operators
Twin Prime Conjecture
  8.2: Prime Numbers and Prime Factorizations

U
union
  5.5: Indexed Families of Sets
universal set
  2.3: Open Sentences and Sets

V
Venn diagram
  5.1: Sets and Operations on Sets

Appendix A: Guidelines for Writing Mathematical Proofs

One of the most important forms of mathematical writing is writing mathematical proofs. The writing of mathematical proofs is an acquired skill and takes a lot of practice. Throughout the textbook, we have introduced various guidelines for writing proofs. These guidelines are in Sections 1.1, 1.2, 3.1, 3.2, 3.3, and 4.1.

Following is a summary of all the writing guidelines introduced in the text. This summary contains some standard conventions that are usually followed when writing a mathematical proof.

1. **Know your audience**. Every writer should have a clear idea of the intended audience for a piece of writing. In that way, the writer can give the right amount of information at the proper level of sophistication to communicate effectively. This is especially true for mathematical writing. For example, if a mathematician is writing a solution to a textbook problem for a solutions manual for instructors, the writing would be brief with many details omitted. However, if the writing was for a students' solution manual, more details would be included.
2. As an example, an exercise in a text might read, "Prove that if x is an odd integer, then x^2 is an odd integer." This could be started as follows:

   Theorem. If x is an odd integer, then x^2 is an odd integer.
   Proof: We assume that x is an odd integer ....
3. **Begin the proof with a statement of your assumptions**. Follow the statement of your assumptions with a statement of what you will prove.

   Proof. We assume that x and y are odd integers and will prove that $x \cdot y$ is an odd integer.
4. **Use the pronoun "we."** If a pronoun is used in a proof, the usual convention is to use "we" instead of "I." The idea is to stress that you and the reader are doing the mathematics together. It will help encourage the reader to continue working through the mathematics. Notice that we started the proof of Theorem 1.8 with "We assume that... ."
5. **Use italics for variables when using a word processor.** When using a word processor to write mathematics, the word processor needs to be capable of producing the appropriate mathematical symbols and equations. The mathematics that is written with a word processor should look like typeset mathematics. This means that variables need to be italicized, boldface is used for vectors, and regular font is used for mathematical terms such as the names of the trigonometric functions and logarithmic functions.

   For example, we do not write sin x or $sin\ x$. The proper way to typeset this is $\sin x$.
6. **Do not use $*$ for multiplication or ^ for exponents**. Leave this type of notation for writing computer code. The use of this notation makes it difficult for humans to read. In addition, avoid using / for division when using a complex fraction.
   For example, it is very difficult to read $(x^3 - 3x^2 + 1/2)/(2x/3 - 7)$; the fraction

   $$\frac{x^3 - 3x^2 + \frac{1}{2}}{\frac{2x}{3} - 7} \tag{Appendix A.1}$$

   is much easier to read.
7. **Use complete sentences and proper paragraph structure**. Good grammar is an important part of any writing. Therefore, conform to the accepted rules of grammar. Pay careful attention to the structure of sentences. Write proofs using **complete sentences** but avoid run-on sentences. Also, do not forget punctuation, and always use a spell checker when using a word processor.
8. **Keep the reader informed**. Sometimes a theorem is proven by proving the contrapositive or by using a proof by contradiction. If either proof method is used, this should be indicated within the first few lines of the proof. This also applies if the result is going to be proven using mathematical induction.

Example

- We will prove this result by proving the contrapositive of the statement.
- We will prove this statement using a proof by contradiction.
- We willassume to the contrary that... .
- We will use mathematical induction to prove this result.

In addition, make sure the reader knows the status of every assertion that is made. That is, make sure it is clearly stated whether an assertion is an assumption of the theorem, a previously proven result, a well-known result, or something from the reader's mathematical background.

9. **Display important equations and mathematical expressions.** Equations and manipulations are often an integral part of the exposition. Do not write equations, algebraic manipulations, or formulas in one column with reasons given in another column (as is often done in geometry texts). Important equations and manipulations should be displayed. This means that they should be centered with blank lines before and after the equation or manipulations, and if one side of an equation does not change, it should not be repeated. For example,

   Using algebra, we obtain

   $$\begin{aligned} x \cdot y &= (2m+1)(2n+1) \\ &= 4mn+2m+2n+1 \\ &= 2(2mn+m+n)+1. \end{aligned} \tag{Appendix A.2}$$

   Since m and n are integers, we conclude that ... .

10. **Equation numbering guidelines.** If it is necessary to refer to an equation later in a proof, that equation should be centered and displayed, and it should be given a number. The number for the equation should be written in paren- theses on the same line as the equation at the right-hand margin.

Example

Since x is an odd integer, there exists an integer n such that

$$x = 2n+1 \tag{Appendix A.3}$$

Later in the proof, there may be a line such as

Then, using the result in equation (A.3), we obtain ... .

Please note that we should only number those equations we will be referring to later in the proof. Also, note that the word "equation" is not capitalized when we are referring to an equation by number. Although it may be appropriate to use a capital "E," the usual convention in mathematics is not to capitalize.

11. **Do not use a mathematical symbol at the beginning of a sentence.**
    For example, we should not write, "Let n be an integer. n is an odd integer provided that ... ." Many people find this hard to read and often have to reread it to understand it. It would be better to write, "An integer n is an odd integer provided that ... ."
12. **Use English and minimize the use of cumbersome** notation. Do not use the special symbols for quantifiers $\forall$ (for all), $\exists$ (there exists), $\ni$ (such that), or $\therefore$ (therefore) in formal mathematical writing. It is often easier to write, and usually easier to read, if the English words are used instead of the symbols. For example, why make the reader interpret

    $$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x+y=0) \tag{Appendix A.4}$$

    where it is possible to write

    For each real number x, there exists a real number y such that $x+y=0$, or more succinctly (if appropriate)

    Every real number has an additive inverse.

13. **Tell the reader when the proof has been completed.** Perhaps the best way to do this is to say outright that, “This completes the proof.” Although it may seem repetitive, a good alternative is to finish a proof with a sentence that states precisely what has been proven. In any case, it is usually good practice to use some “end of proof symbol” such as ■.
14. **Keep it simple**. It is often difficult to understand a mathematical argument no matter how well it is written. Do not let your writing help make it more difficult for the reader. Use simple, declarative sentences and short paragraphs, each with a simple point.
15. **Write a first draft of your proof and then revise it**. Remember that a proof is written so that readers are able to read and understand the reasoning in the proof. Be clear and concise. Include details but do not ramble. Do not be satisfied with the first draft of a proof. Read it over and refine it. Just like any worthwhile activity, learning to write mathematics well takes practice and hard work. This can be frustrating. Everyone can be sure that there will be some proofs that are difficult to construct, but remember that proofs are a very important part of mathematics. So work hard and have fun.

Appendix B: Answers for the Progress Checks

Section 1.1

Progress Check 1.2

1. This proposition is false. A counterexample is $a = 2$ and $b = 1$. For these values, $(a+b)^2 = 9$ and $a^2 + b^2 = 5$.
2. This proposition is true, as we can see by using $x = 3$ and $y = 7$. We could also use $x = -2$ and $y = 9$. There are many other possible choices for x and y.
3. This proposition appears to be true. Anytime we use an example where x is an even integer, the number x^2 is an even integer. However, we cannot claim that this is true based on examples since we cannot list all of the examples where x is an even integer.
4. This proposition appears to be true. Anytime we use an example where x and y are both integers, the number $x \cdot y$ is an odd integer. However, we cannot claim that this is true based on examples since we cannot list all of the examples where both x and y are odd integers.

Progress Check 1.4

1. (a) This does not mean the conditional statement is false since when $x = -3$, the hypothesis is false, and the only time a conditional statement is false is when the hypothesis is true and the conclusion is false.
   (b) This does not mean the conditional statement is true since we have not checked all positive real numbers, only the one where $x = 4$.
   (c) All examples should indicate that the conditional statement is true.
2. The number $(n2 - n + 41)$ will be a prime number for all examples of \(n\) that are less than 41. However, when $n = 41$, we get

$$\begin{aligned} n^2 - n + 41 &= 41^2 - 41 + 41 \\ n^2 - n + 41 &= 41^2 \end{aligned} \tag{Appendix B.1}$$

   So in the case where $n = 41$, the hypothesis is true (41 is a positive integer) and the conclusion is false (41^2 is not prime). Therefore, 41 is a counterexample that shows the conditional statement is false. There are other counterexamples (such as $n = 42$, $n = 45$, and $n = 50$), but only one counterexample is needed to prove that the statement is false.

Progress Check 1.5

1. We can conclude that this function is continuous at 0.
2. We can make no conclusion about this function from the theorem.
3. We can make no conclusion about this function from the theorem.
4. We can conclude that this function is not differentiable at 0.

Progress Check 1.7

1. The set of rational numbers is closed under addition since $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.
2. The set of integers is not closed under division. For example, $\frac{2}{3}$ is not an integer.
3. The set of rational numbers is closed under subtraction since $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}$.

Section 1.2

Progress Check 1.10

All examples should indicate the proposition is true. Following is a proof.

Proof. We assume that m is an odd integer and will prove that $(3m^2 + 4m + 6)$. Since m is an odd integer, there exists an integer k such that $mD = 2k + 1$. Substituting this into the expression $(3m^2 + 4m + 6)$ and using algebra, we obtain

$$\begin{aligned} 3m^2 + 4m + 6 &= 3(2k+1)^2 + 4(2k+1) + 6 \\ &= (12k^2 + 12k + 3) + (8k + 4) + 6 \\ &= 12k^2 + 20k + 13 \\ &= 12k^2 + 20k + 12 + 1 \\ &= 2(6k^2 + 10k + 6) + 1 \end{aligned}$$

Progress Check 1.11

Proof. We let m be a real number and assume that m, $m+1$, and $m+2$ are the lengths of the three sides of a right triangle. We will use the Pythagorean Theorem to prove that $m=3$. Since the hypotenuse is the longest of the three sides, the Pythagorean Theorem implies that $m^2+(m+1)^2=(m+2)^2$. We will now use algebra to rewrite both sides of this equation as follows:

$$\begin{aligned} m^2+(m^2+2m+1) &= m^2+4m+4 \\ 2m^2+2m+1 &= m^2+4m+4 \end{aligned}$$

The last equation is a quadratic equation. To solve for m, we rewrite the equation in standard form and then factor the left side. This gives

$$\begin{aligned} m^2-2m-3 &= 0 \\ (m-3)(m+1) &= 0 \end{aligned}$$

The two solutions of this equation are $m=3$ and $m=-1$. However, since m is the length of a side of a right triangle, m must be positive and we conclude that $m=3$. This proves that if m, $m+1$, and $m+2$ are the lengths of the three sides of a right triangle, then $m=3$.

Section 2.1

Progress Check 2.1

1. Whenever a quadrilateral is a square, it is a rectangle, or a quadrilateral is a rectangle whenever it is a square.
2. A quadrilateral is a square only if it is a rectangle.
3. Being a rectangle is necessary for a quadrilateral to be a square.
4. Being a square is sufficient for a quadrilateral to be a rectangle.

Progress Check 2.2

P	Q	$P \wedge \urcorner Q$	$\urcorner(P \wedge Q)$	$\urcorner P \wedge \urcorner Q$	$\urcorner P \vee \urcorner Q$
T	T	F	F	F	F
T	F	T	T	F	T
F	T	F	T	F	T
F	F	F	T	T	T

Statements (2) and (4) have the same truth table.

Progress Check 2.4

P	$\urcorner P$	$P \vee \urcorner P$	$P \wedge \urcorner P$
T	F	T	F
F	T	T	F

P	Q	$P \vee Q$	$P \to (P \vee Q)$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	T

Section 2.2

Progress Check 2.7

1. Starting with the suggested equivalency, we obtain

$$\begin{aligned}(P \wedge \urcorner Q) \to R &\equiv \urcorner(P \wedge \urcorner Q) \vee R \\ &\equiv (\urcorner P \vee \urcorner(\urcorner Q)) \vee R \\ &\equiv \urcorner P \vee (Q \vee R) \\ &\equiv P \to (Q \vee R)\end{aligned} \tag{Appendix B.2}$$

2. For this, let P be,“3 is a factor of $a \cdot b$,” let Q be, “is a factor of a,” and let R be, “3 is a factor of b.” Then the stated proposition is written in the form $P \to (Q \vee R)$. Since this is logically equivalent to $(P \wedge \urcorner Q) \to R$, if we prove that

   if 3 is a factor of $a \cdot b$ and 3 is not a factor of a, then 3 is a factor of b, then we have proven the original proposition.

Section 2.3

Progress Check 2.9

1. $10 \in A$, $22 \in A$, $13 \notin A$, $0 \in A$, $-12 \notin A$
2. $A = B, A \subseteq B, B \subseteq A, A \subseteq C, A \subseteq D, B \subseteq C, B \subseteq D$

Progress Check 2.11

1. (a) Two values of x for which $P(x)$ is false are $x = 3$ and $x = -4$.
   (b) The set of all x for which $P(x)$ is true is the set {-2, -1, 0, 1, 2}.
2. (a) Two examples for which $R(x, y, z)$ is false are: $x = 1, y = 1, z = 1$ and $x = 3$, $y = -1$, $z = 5$.
   (b) Two examples for which $R(x, y, z)$ is true are: $x = 3, y = 4, z = 5$ and $x = 5, y = 12, z = 13$.

Progress Check 2.13

1. The truth set is the set of all real numbers whose square is less than or equal to 9. The truth set is $\{x \in \mathbb{R} \mid x^2 \le 9\} = \{x \in \mathbb{R} \mid -3 \le x \le 3\}$.
2. The truth set is the set of all integers whose square is less than or equal to 9. The truth set is {-3, -2, -1, 0, 1, 2, 3}.
3. The truth sets in Parts (1) and (2) equal are not equal. One purpose of this progress check is to show that the truth set of a predicate depends on the predicate and on the universal set.

Progress Check 2.15

$A = \{4n - 3 \mid n \in \mathbb{N}\} = \{x \in \mathbb{N} \mid x = 4n - 3 \text{ for some natural number } n\}$.

\(B = \{-2n\ |\ \text{n is a nonnegative integer\}.\)

$C = \{(\sqrt{2})^{2m-1} \mid m \in \mathbb{N}\} = \{(\sqrt{2})^n \mid n \text{ is an odd natural number}\}$.

$D = \{3^n \mid n \text{ is a nonnegative integer}\}$.

Section 2.4

Progress Check 2.18

1. - For each real number a, $a + 0 = a$.
   - $(\exists a \in \mathbb{R})(a + 0 \ne a)$.
   - There exists a real number a such that $a + 0 \ne a$.
2. - For each real number x, sin (2x) = 2(sin x)(cos x).
   - $(\exists x \in \mathbb{R})$ (sin (2x) $\ne$ 2 (sin x) (cos x)).
   - There exists a real number x such that sin (2x) $\ne$ 2 (sin x) (cos x).
3. - For each real number x, $\tan^2 x + 1 = \sec^2 x$.
   - $(\exists x \in \mathbb{R})(\tan^2 x + 1 \ne \sec^2 x)$.
   - There exists a real number x such that $\tan^2 x + 1 \ne \sec^2 x$.
4. - There exists a rational number x such that $x^2 - 3x - 7 = 0$.
   - $(\forall x \in \mathbb{Q})(x^2 - 3x - 7 \ne 0)$.
   - For each rational number x, $x^2 - 3x - 7 \ne 0$.
5. - There exists a real number x such that $x^2 + 1 = 0$.
   - $(\forall x \in \mathbb{R})(x^2 + 1 \ne 0)$.

- For each real number x, $x^2+1 \neq 0$.

Progress Check 2.19

1. A counterexample is $n=4$ since $4^2+4+1=21$, and 21 is not prime.
2. A counterexample is $x=\frac{1}{4}$ since $\frac{1}{4}$ is positive and $2(\frac{1}{4})^2=\frac{1}{8}$ and $\frac{1}{8} \leq \frac{1}{4}$.

Progress Check 2.20

1. An integer n is a multiple of 3 provided that $\exists k \in \mathbb{Z})(n=3k)$.
4. An integer n is not a multiple of 3 provided that $\forall k \in \mathbb{Z})(n \neq 3k)$.
5. An integer n is not a multiple of 3 provided that for every integer k, $n \neq 3k$.

Progress Check 2.21

- $(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x+y \neq 0)$.
- There exist integers x and y such that $x+y \neq 0$.

Section 3.1

Progress Check 3.2

2. For each example in Part (1), the integer a divides the sum $b+c$.
3. Conjecture: For all integers a, b, and c with $a \neq 0$, if a divides b and a divides c, then a divides $b+c$.
4. A Know-show table for a proof of the conjecture in Part (3).

Step	**Know**	**Reason**
P	$a \mid b$ and $a \mid c$	Hypothesis
$P1$	$(\exists s \in \mathbb{Z})(b=a \cdot s)$ $(\exists t \in \mathbb{Z})(c=a \cdot t)$	Definition of "divides"
$P2$	$b+c=as+at$	Substituting for b and c
$P3$	$b+c=a(s+t)$	Distributive property
$Q1$	$s+t$ is an integer	$\mathbb{Z}$ is closed under addition
Q	$a \mid (b+c)$	Definition of "divides"
Step	**Show**	**Reason**

Progress Check 3.3

A counterexample for this statement will be values of a and b for which 5 divides a or 5 divides b, and 5 does not divide $5a+b$. One counterexample for the statement is $a=5$ and $b=1$. For these values, the hypothesis is true since 5 divides a and the conclusion is false since $5a+b=26$ and 5 does not divide 26.

Progress Check 3.4

1. Some integers that are congruent to 5 modulo 8 are -11, -3, 5, 13, and 21.
2. \(\{x \in \mathbb{Z}\ |\ x \equiv 5\text{ (mod 8)\} = \{..., -19, -11, -3, 5, 13, 21, 29, ...\}\).
3. For example, -3 + 5 = 2, -11 + 29 = 18, 13 + 21 = 34.
4. If we subtract 2 from any of the sums obtained in Part (3), the result will be a multiple of 8. This means that the sum is congruent to 2 modulo 8. For example, $2-2=0$, $18-2=16$, $34-2=32$.

Progress Check 3.6

1. To prove that 8 divides $(a+b-2)$, we can prove that there exists an integer q such that $(a+b-2=8q)$.
2. Since 8 divides $(a-5)$ and $(b-5)$, there exist integers k and m such that $a-5-8k$ and $b-5=8m$.
3. $a=5+8k$ and $b=5+8m$.
4. $a+b-2=(5+8k)+5+8m)-2=8+8k+8m=8(1+k+m)$.

5. ***Proof.*** Let a and b be integers and assume that $a \equiv 5 \pmod 8$ and $b \equiv 5 \pmod 8$. We will prove that $(a+b) \equiv 2$ (mod 8\). Since 8 divides $(a-5)$ and $(b-5)$, there exist integers k and m such that $a-5=8k$ and $b-5=8m$. We then see that \[\begin{array} {a + b - 2} &= & {(5 + 8k) + (5 + 8m) - 2] \ {} &= & {8 + 8k + 8m} \ {} &= & {8(1 + k + m)} \end{array}\] By the closure properties of the integers, $(1+k+m)$ is an integer and so the last equation proves that 8 divides $(a+b-2)$ and hence, $(a+b) \equiv 2 \pmod 8$. This proves that if $a \equiv 5 \pmod 8$ and $b \equiv 5 \pmod 8$, then $(a+b) \equiv 2 \pmod 8$.

Section 3.2

Progress Check 3.8

1. For all real numbers a and b, if $ab=0$, then $a=0$ or $b=0$.
2. For all real numbers a and b, if $ab=0$ and $a \neq 0$, $b=0$
3. This gives

$$\frac{1}{a}(ab) = \frac{1}{a} \cdot 0. \tag{Appendix B.3}$$

We now use the associative property on the left side of this equation and simplify both sides of the equation to obtain

$$\begin{array}{rcl} (\frac{1}{a} \cdot a)b & = & 0 \\ 1 \cdot b & = & 0 \\ b & = & 0 \end{array} \tag{Appendix B.4}$$

Therefore, $b=0$ and this completes the proof of a statement that is logically equivalent to the contrapositive. Hence, we have proved the proposition.

Section 3.3

Progress Check 3.15

1. There exists a real number x such that x is irrational and $\sqrt[3]{x}$ is rational.
2. There exists a real number x such that $x+\sqrt{2}$ is rational and $(-x+\sqrt{2})$ is rational.
3. There exist integers a and b such that 5 divides ab and 5 does not divide a and 5 does not divide b.
4. There exist real numbers a and b such that $a>0$ and $b>0$ and $\dfrac{2}{a}+\dfrac{2}{b}=\dfrac{4}{a+b}$.

Progress Check 3.16

1. Some integers that are congruent to 2 modulo 4 are -6. -2, 2, 6, 10, and some integers that are congruent to 3 modulo 6 are: -9, -3, 3, 9, 15. There are no integers that are in both of the lists.
2. For this proposition, it is reasonable to try a proof by contradiction since the conclusion is stated as a negation.
3. Proof. We will use a proof by contradiction. Let $n \in \mathbb{Z}$ and assume that $n \equiv 2 \pmod 4$ and that $n \equiv 3 \pmod 6$. Since $n \equiv 2$ (mod 4), we know that 4 divides $n-2$. Hence, there exists an integer k such that

$$n-2=4k. \tag{Appendix B.5}$$

We can also use the assumption that $n \equiv 3 \pmod 6$ to conclude that 6 divides $n-3$ and that there exists an integer m such that

$$n-3=6m. \tag{Appendix B.6}$$

If we now solve equations (B.5) and (B.6) for n and set the two expressions equal to each other, we obtain

$$4k+2=6m+3. \tag{Appendix B.7}$$

However, this equation can be rewritten as

$$2(2k+1)=2(3m+1)+1. \tag{Appendix B.8}$$

Since $2k+1$ is an integer and $3m+1$ is an integer, this last equation is a contradiction since the left side is an even integer and the right side is an odd integer. Hence, we have proven that if $n \equiv 2$ (mod 4), then $n \equiv 3$ (mod 6).

Progress Check 3.18

1. $x^2+y^2=(2m+1)^2+(2n+1)^2=2(2m^2+2m+2n^2+2n+1)$.
2. Using algebra to rewrite the last equation, we obtain

$$4m^2+4m+4n^2+4n+2=4k^2. \tag{Appendix B.9}$$

If we divide both sides of this equation by 2, we see that $2m^2+2m+2n^2+2n+1=2k^2$ or

$$2(m^2+m+n^2+n)+1=2k^2. \tag{Appendix B.10}$$

However, the left side of the last equation is an odd integer and the right side is an even integer. This is a contradiction, and so we have proved that for all integers x and y, if x and y are odd integers, then there does not exist an integer z such that x^2+y^2 $=z^2$.

Section 3.4

Progress Check 3.21

Proposition. For each integer n, n^2-5n+7 is an odd integer.

Proof. Let n be an integer. We will prove that n^2-5n+7 is an odd integer by examining the case where n is even and the case where n is odd.

In the case where n is even, there exists an integer m such that $n=2m$. So in this case,

$$\begin{aligned} n^2-5n+7 &= (2m^2)-5(2m)+7 \\ &= 4m^2-10m+6+1 \\ &= 2(2m^2-5m+3)+1. \end{aligned}$$

Since $(2m^2-5m+3)$ is an integer, the last equation shows that if n is even, then n^2-5n+7 is odd.

In the case where n is odd, there exists an integer m such that $n=2m+1$. So in this case,

$$\begin{aligned} n^2-5n+7 &= (2m+1)^2-5(2m+1)+7 \\ &= 4m^2-14m+3 \\ &= 2(2m^2-7m+1)+1. \end{aligned}$$

Since $(2m^2-7m+1)$ is an integer, the last equation shows that if n is odd, then n^2-5n+7 is odd. Hence, by using these two cases, we have shown that for each integer n, n^2-5n+7 is an odd integer.

Progress Check 3.24

1. |4.3| = 4.3 and |-π| = π
2. (a) $t=12$ or $t=-12$
   (b) $t+3=5$ or $t+3=-5$. So $t=2$ or $t=-8$.
   (c) $t-4=\dfrac{1}{5}$ or $t-4=-\dfrac{1}{5}$. So $t=\dfrac{21}{5}$ or $t=\dfrac{19}{5}$.
   (d) $3t-4=8$ or $3t-4=-8$. So $t=4$ or $t=-\dfrac{4}{3}$.

Section 3.5

Progress Check 3.26

1. (a) The possible remainders are 0, 1, 2, and 3.
   (b) The possible remainders are 0, 1, 2, 3, 4, 5, 6, 7, and 8.

   (a) $17=5\cdot 3+2$
   (b) $-17=(-6)\cdot 3+1$

(c) $73 = 10 \cdot 7 + 3$
(d) $-73 = (-11) \cdot 7 + 4$
(e) $436 = 16 \cdot 27 + 4$
(f) $539 = 4 \cdot 110 + 99$

Progress Check 3.29

Proof. Let n be a natural number and let a, b, c and d be integers.We assume that $a \equiv b$ (mod n) and $c \equiv d$ (mod n) and will prove that $(a+c) \equiv (b+d)$ (mod n). Since $a \equiv b$ (mod n) and $c \equiv d$ (mod n), n divides $a-b$ and $c-d$ and so there exist integers k and q such that $a-b=nk$ and $c-d=nq$. We can then write $a=b+nk$ and $c=d+nq$ and obtain

$$\begin{array}{rcl} a+c & = & (b+nk)+(d+nq) \\ & = & (b+d)+n(k+q) \end{array}.$$

By subtracting $(b+d)$ from both sides of the last equation, we see that

$(a+c)-(b+d)=n(k+q)$.

Since $(k+q)$ is an integer, this proves that n divides $(a+c)-(b+d)$, and hence, we can conclude that $(a+c) \equiv (b+d)$ (mod n).

Progress Check 3.34

Case 2. ($a \equiv 2$ (mod 5)). In this case, we use Theorem 3.28 to conclude that

$$a^2 \equiv 2^2 \text{ (mod 5) or } a^2 \equiv 4 \text{ (mod 5).}$$

This proves that if $a \equiv 2$ (mod 5), then $a^2 \equiv 4$ (mod 5).

Case 3. ($a \equiv 3$ (mod 5)). In this case, we use Theorem 3.28 to conclude that

$$a^2 \equiv 3^2 \text{ (mod 5) or } a^2 \equiv 9 \text{ (mod 5).}$$

We also know that $9 \equiv 4$ (mod 5). So we have $a^2 \equiv 9$ (mod 5) and $9 \equiv 4$ (mod 5), and we can now use the transitive property of congruence (Theorem 3.30) to conclude that $a^2 \equiv 4$ (mod 5). This proves that if $a \equiv 3$ (mod 5), then $a^2 \equiv 4$ (mod 5).

Section 4.1

Progress Check 4.1

1. It is not possible to tell if $1 \in T$ and $5 \in T$.
2. True.
3. True. The contrapositive is, "If $2 \in T$, then $5 \in T$," which is true.
4. True.
5. False. If $k \in T$, then $k+1 \in T$.
6. True, since "k \notin t\) OR $k+1 \in T$" is logically equivalent to "If $k \in T$, then $k+1 \in T$."
7. It is not possible to tell if this is true. It is the converse of the conditional statement, “For each integer k, if $k \in T$, then $k+1 \in T$."
8. True. This is the contrapositive of the conditional statement, “For each integer k, if $k \in T$, then $k+1 \in T$."

Progress Check 4.3

Proof. Let $P(n)$ be the predicate, "$1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$." For basis step, notice that the equation $1 = \dfrac{1(1+1)}{2}$ shows that $P(1)$ is true. Now let k be a natural number an assume that $P(k)$ is true. That is, assume that

$$1+2+3+\cdots+k = \frac{k(k+1)}{2}. \tag{Appendix B.11}$$

We now need to prove that $P(k+1)$ is true or that

$$1+2+3+\cdots+k+(k+1) = \frac{(k+1)(k+2)}{2}. \tag{Appendix B.12}$$

By adding $(k+1)$ to both sides of equation (B.11), we see that

$$\begin{aligned} 1+2+3+\cdots+k+(k+1) &= \frac{k(k+1)}{2}+(k+1) \\ &= \frac{k(k+1)+2(k+1)}{2} \\ &= \frac{k^2+3k+2}{2} \\ &= \frac{(k+1)(k+2)}{2}. \end{aligned}$$

By comparing the last equation to equation (2), we see that we have proved that if $P(k)$ is true, then $P(k+1)$ is true, and the inductive step has been established. Hence, by the Principle of Mathematical Induction, we have proved that for each integer n, $1+2+3+\cdots+n=\dfrac{n(n+1)}{2}$.

Progress Check 4.5

For the inductive step, let k be a natural number and assume that $P(k)$ is true. That is, assume that $5^k \equiv 1$ (mod 4).

1. To prove that $P(k+1)$ is true, we must prove $5^{k+1} \equiv 1$ (mod 4).
2. Since $5^{k+1} = 5 \cdot 5^k$, we multiply both sides of the congruence $5^k \equiv 1$ (mod 4) by 5 and obtain

$$5 \cdot 5^k \equiv 5 \cdot 1 \pmod 4 \text{ or } \qquad 5^{k+1} \equiv 5 \pmod 4. \qquad \text{(Appendix B.13)}$$

3. Since $5^{k+1} \equiv 5$ (mod 4) and we know that $5 \equiv 1$ (mod 4), we can use the transitive property of congruence to obtain $5^{k+1} \equiv 1$ (mod 4). This proves that if $P(k)$ is true, then $P(k+1)$ is true, and hence, by the Principle of Mathematical Induction, we have proved that for each natural number n, $5^n \equiv 1$ (mod 4).

Section 4.2

Progress Check 4.8

1. For each natural number n, if $n \geq 3$, then $3^n > 1 + 2^n$.
2. For each natural number n, if $n \geq 6$, then $2^n > (n+1)^2$.
3. For each natural number n, if $n \geq 6$, then $(1+\dfrac{1}{n})^n > 2.5$.

Progress Check 4.10

Construct the following table and use it to answer the first two questions. The table shows that $P(3)$, $P(5)$, and $P(6)$ are true. We can also see that $P(2)$, $P(4)$, and $P(7)$ are false. It also appears that if $n \in \mathbb{N}$ and $n \geq 8$, then $P(n)$ is true.

x	0	1	2	3	4	0	1	2	0	1	1
y	0	0	0	0	0	1	1	1	2	2	3
$3x+5y$	0	3	6	9	12	5	8	11	10	13	18

The following proposition provides answers for Problems (3) and (4).

Proposition 4.11. For all natural numbers n with $n \geq 8$, there exist non-negative integers x and y such that $n = 3x + 5y$.

Proof. (by mathematical induction) Let $\mathbb{Z}^* = \{x \in \mathbb{Z} \mid x \geq 0\}$, and for each natural number n, let $P(n)$ be, "there exist $x, y \in \mathbb{Z}^*$ such that $n = 3x + 5y$."

Basis Step: Using the table above, we see that $P(8)$, $P(9)$, and $P(10)$ are true.

Inductive Step: Let $k \in \mathbb{N}$ with $k \geq 13$. assume that $P(8)$, $P(9)$, ..., $P(k)$ are true. Now, notice that

$$k+1 = 3 + (k-2).$$

Since $k \geq 10$, we can conclude that $k-2 \geq 8$ and hence $P(k-2)$ is true. Therefore, there exist non-negative integers u and v such that $k-2 = (3u+5v)$. Using this equation, we see that

Illegal pream-token (k)

Hence, we can conclude that $P(k+1)$ is true. This proves that if $P(8)$, $P(9)$, ..., $P(k)$ are true, then $P(k+1)$ is true. Hence, by the Second Principle of Mathematical Induction, for all natural numbers n with $n \geq 8$, there exist nonnegative integers x and y such that

$n = 3x + 5y$.

Section 4.3

Progress Check 4.12

Proof. We will use a proof by induction. For each natural number n, we let $P(n)$ be,

f_{3n} is an even natural number.

Since $f_3 = 2$, we see that $P(1)$ is true and this proves the basis step.

For the inductive step, we let k be a natural number and assume that $P(k)$ is true. That is, assume that f_{3k} is an even natural number. This means that there exists an integer m such that

$$f_{3k} = 2m. \tag{Appendix B.14}$$

We need to prove that $P(k+1)$ is true or that $f_{3(k+1)}$ is even. Notice that $3(k+1) = 3k+3$ and, hence, \(f_{3(k + 1) = f_{3k + 3}\). We can now use the recursion formula for the Fibonacci numbers to conclude that

$$f_{3k+3} = f_{3k+2} + f_{3k+1}.$$

Using the recursion formula again, we get $f_{3k+2} = f_{3k+1} + f_{3k}$. Putting this all together, we see that

$$\begin{aligned} f_{3(k+1)} &= f_{3k+3} \\ &= f_{3k+2} + f_{3k+1} \\ &= (f_{3k+1} + f_{3k}) + f_{3k+1} \\ &= 2f_{3k+1} + f_{3k}. \end{aligned} \tag{Appendix B.15}$$

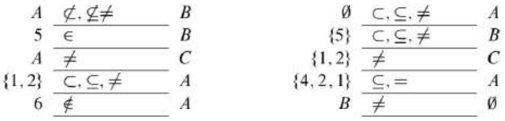
We now substitute the expression for f_{3k} in equation (B.14) into equation (B.15). This gives

$$\begin{aligned} f_{3(k+1)} &= 2f_{3k+1} + 2m \\ f_{3(k+1)} &= 2(f_{3k+1} + m) \end{aligned} \tag{Appendix B.16}$$

This preceding equation shows that $f_{3(k+1)}$ is even. Hence it has been proved that if $P(k)$ is true, then $P(k+1)$ is true and the inductive step has been established. By the Principle of Mathematical Induction, this proves that for each natural number n, the Fibonacci number f_{3n} is an even natural number.

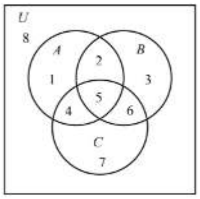
Section 5.1

Progress Check 5.3



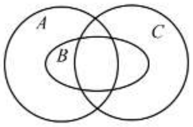
A	$\not\subset, \not\subseteq \neq$	B	$\emptyset$	$\subset, \subseteq, \neq$	A
5	$\in$	B	$\{5\}$	$\subset, \subseteq, \neq$	B
A	$\neq$	C	$\{1, 2\}$	$\neq$	C
$\{1, 2\}$	$\subset, \subseteq, \neq$	A	$\{4, 2, 1\}$	$\subseteq, =$	A
6	$\notin$	A	B	$\neq$	$\emptyset$

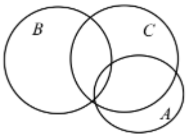
Progress Check 5.4

1. 

   Using the standard Venn diagram for three sets shown above:

   (a) For the set $(A \cap B) \cap C$, region 5 is shaded.
   (b) For the set $(A \cap B) \cup C$, the regions 2, 4, 5, 6, 7 are shaded.
   (c) For the set $(A^c \cup B)$, the regions 2, 3, 5, 6, 7, 8 are shaded.
   (d) For the set $(A^c \cap (B \cup C))$, the regions 3, 6, 7 are shaded.

2. 

3. 

Section 5.2

Progress Check 5.8

$A = \{x \in \mathbb{Z} \mid x \text{ is multiple of } 9\}$ and $B = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 3\}$.

1. The set A is a subset of B. To prove this, we let $x \in A$. Then there exists an integer m such that $x = 9m$, which can be written as

$$x = 3(3m). \tag{Appendix B.17}$$

   Since $3m \in \mathbb{Z}$, the last equation proves that x is a multiple of 3 and so $x \in B$. Therefore, $A \subseteq B$.
2. The set A is not equal to the set B. We note that $3 \in B$ but $3 \notin A$. Therefore, $B \not\subseteq A$ and, hence, $A \neq B$.

Progress Check 5.9

Step	Know	Reason
P	$A \subseteq B$	Hypothesis
$P1$	Let $x \in B^c$.	Choose an arbitrary element of B^c.
$P2$	If $x \in A$, then $x \in B$.	Definition of "subset"
$P3$	If $x \notin B$, then $x \notin A$.	Contrapositive
$P4$	If $x \in B^c$, then $x \in A^c$.	Step $P3$ and definition of "complement"
$Q2$	The element x is in A^c.	Step $P1$ and $P4$
$Q1$	Every element of B^c is an element of A^c.	The choose-an-element method with Steps $P1$ and $Q2$.
Q	$B^c \subseteq A^c$	Definition of "subset"

Progress Check 5.12

Proof. Let A and B be subsets of some universal set. We will prove that $A - B = A \cap B^c$ by proving that each set is a subset of the other set. We will first prove that $A - B \subseteq A \cap B^c$. Let $x \in A - B$. We then know that $x \in A$ and $x \notin B$. However, $x \notin B$ implies that $x \in B^c$. Hence, $x \in A$ and $x \in B^c$, which means that $x \in A \cap B^c$. This proves that $A - B \subseteq A \cap B^c$.

To prove that $A \cap B^c \subseteq A - B$, we let $y \in A \cap B^c$. This means that $y \in A$ and $y \in B^c$, and hence, $y \in A$ and $y \notin B$. Therefore, $y \in A - B$ and this proves that $A \cap B^c \subseteq A - B$. Since we have proved that each set is a subset of the other set, we have proved that $A - B = A \cap B^c$.

Progress Check 5.15

Proof. Let $A = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod{12}\}$ and $B = \{y \in \mathbb{Z} \mid y \equiv 2 \pmod{8}\}$. We will use a proof by contradiction to prove that $A \cap B = \emptyset$. So we assume that $A \cap B \neq \emptyset$ and let $x \in A \cap B$. We can then conclude that $x \equiv 3 \pmod{12}$ and that $x \equiv 2$ (mod 8). This means that there exist integers m and n such that

$$x = 3 + 12m \text{ and } x = 2 + 8n.$$

By equating these two expressions for x, we obtain $3+12m=2+8n$, and this equation can be rewritten as $1=8n-12m$. This is a contradiction since 1 is an odd integer and $8n-12m$ is an even integer. We have therefore proved that $A\cap B=\emptyset$.

Section 5.3

Progress Check 5.19

1. In our standard configuration for a Venn diagram with three sets, regions 1, 2, 4, 5, and 6 are the shaded regions for both $A\cup(B\cap C)$ and $(A\cup B)\cap(A\cup C)$.
2. Based on the Venn diagrams in Part (1), it appears that $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$.

Progress Check 5.21

1. Using our standard configuration for a Venn diagram with three sets, regions 1, 2, and 3 are the regions that are shaded for both $(A\cup B)-C$ and $(A-C)\cup(B-C)$.
2. $$\begin{aligned} (A\cup B)-C &= (A\cup B)\cap C^c && \text{(Theorem 5.20)}\\ &= C^c\cap(A\cup B) && \text{(Commutative Property)}\\ &= (C^c\cap A)\cup(C^c\cap B) && \text{(Distributive Property)}\\ &= (A\cap C^c)\cup(B\cap C^c) && \text{(Commutative Property)}\\ &= (A-C)\cup(B-C) && \text{(Theorem 5.20)} \end{aligned}$$

Section 5.4

Progress Check 5.23

1. Let $A=\{1,2,3\}$, $T=\{1,2\}$, $B=\{a,b\}$, and $C=\{a,c\}$.

   (a) $A\times B=\{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}$
   (b) $T\times B=\{(1,a),(1,b),(2,a),(2,b)\}$
   (c) $A\times C=\{(1,a),(1,c),(2,a),(2,c),(3,a),(3,c)\}$
   (d) $A\times(B\cap C)=\{(1,a),(2,a),(3,a)\}$
   (e) $(A\times B)\cap(A\times C)=\{(1,a),(2,a),(3,a)\}$
   (f) $A\times(B\cup C)=\{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c),(3,a),(3,b),(3,c)\}$
   (g) $(A\times B)\cup(A\times C)=\{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c),(3,a),(3,b),(3,c)\}$
   (h) $A\times(B-C)=\{(1,b),(2,b),(3,b)\}$
   (i) $(A\times B)-(A\times C)=\{(1,b),(2,b),(3,b)\}$
   (j) $B\times A=\{(a,1),(b,1),(a,2),(b,2),(a,3),(b,3)\}$
2. $$\begin{array}{ll} T\times B\subseteq A\times B & A\times(B\cup C)=(A\times B)\cup(A\times C)\\ A\times(B\cap C)=(A\times B)\cap(A\times C) & A\times(B-C)=(A\times B)-(A\times C) \end{array}$$

Progress Check 5.24

1. (a) $A\times B=\{(x,y)\in\mathbb{R}\times\mathbb{R}\mid 0\le x\le 2 \text{ and } 2\le y<4\}$
   (b) $T\times B=\{(x,y)\in\mathbb{R}\times\mathbb{R}\mid 1<x<2 \text{ and } 2\le y<4\}$
   (c) $A\times C=\{(x,y)\in\mathbb{R}\times\mathbb{R}\mid 0\le x\le 2 \text{ and } 3<y\le 6\}$
   (d) $A\times(B\cap C)=\{(x,y)\in\mathbb{R}\times\mathbb{R}\mid 0\le x\le 2 \text{ and } 3<y<4\}$
   (e) $(A\times B)\cap(A\times C)=\{(x,y)\in\mathbb{R}\times\mathbb{R}\mid 0\le x\le 2 \text{ and } 3<y<4\}$
   (f) $A\times(B\cup C)=\{(x,y)\in\mathbb{R}\times\mathbb{R}\mid 0\le x\le 2 \text{ and } 2\le y\le 5\}$
   (g) $(A\times B)\cup(A\times C)=\{(x,y)\in\mathbb{R}\times\mathbb{R}\mid 0\le x\le 2 \text{ and } 2\le y\le 5\}$
   (h) $A\times(B-C)=\{(x,y)\in\mathbb{R}\times\mathbb{R}\mid 0\le x\le 2 \text{ and } 2\le y\le 3\}$
   (i) $(A\times B)-(A\times C)=\{(x,y)\in\mathbb{R}\times\mathbb{R}\mid 0\le x\le 2 \text{ and } 2\le y\le 3\}$
   (j) $B\times A=\{(x,y)\in\mathbb{R}\times\mathbb{R}\mid 2\le x<4 \text{ and } 0\le y\le 2\}$
2. $T\times B\subseteq A\times B$
   $A\times(B\cap C)=(A\times C)\cap(A\times C)$
   $A\times(B\cup C)=(A\times C)\cup(A\times C)$
   $A\times(B-C)=(A\times C)-(A\times C)$

Section 5.5

Progress Check 5.26

1. $\bigcup_{j=1}^{6} A_j = \{1, 2, 3, 4, 5, 6, 9, 16, 25, 36\}$
2. $\bigcap_{j=1}^{6} A_j = \{1\}$
3. $\bigcup_{j=3}^{6} A_j = \{3, 4, 5, 6, 9, 16, 25, 36\}$
4. $\bigcap_{j=3}^{6} A_j = \{1\}$
5. $\bigcup_{j=1}^{\infty} A_j = \mathbb{N}$
6. $\bigcap_{j=1}^{\infty} A_j = \{1\}$

Progress Check 5.27

1. $A_1 = \{7, 14\}$, $A_2 = \{10, 12\}$, $A_3 = \{10, 12\}$, $A_4 = \{8, 14\}$.
2. The statement is false. For example, $2 \neq 3$ and $A_2 = A_3$.
3. The statement is false. For example, $1 \neq -1$ and $B_1 = B_{-1}$.

Progress Check 5.29

1. Since $\bigcup_{\alpha \in \mathbb{R}^+} A_\alpha = (-1, \infty)$, $(\bigcup_{\alpha \in \mathbb{R}^+} A_\alpha)^c = (-\infty, 1]$.
2. $\bigcap_{\alpha \in \mathbb{R}^+} A_\alpha^c = (-\infty, -1]$.
3. Since $\bigcap_{\alpha \in \mathbb{R}^+} A_\alpha = (-1, 0]$, $(\bigcap_{\alpha \in \mathbb{R}^+} A_\alpha)^c = (-\infty, 1] \cup (0, \infty)$.
4. $\bigcup_{\alpha \in \mathbb{R}^+} A_\alpha^c = (-\infty, -1] \cup (0, \infty)$.

Progress Check 5.32

All three families of sets ($\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ are disjoint families of sets. One the family $\mathcal{A}$ is a pairwise disjoint family of sets.

Section 6.1

Progress Check 6.1

1. $f(-3) = 24$
   $f(\sqrt{8}) = 8 - 5\sqrt{8}$
2. $g(2) = -6$, $g(-2) = 14$
3. {-1, 6}
4. {-1, 6}
5. $\{\dfrac{5 + \sqrt{33}}{2}, \dfrac{5 - \sqrt{33}}{2}\}$
6. $\emptyset$

Progress Check 6.2

1. (a) The domain of the function f is the set of all people.
   (b) A codomain for the function f is the set of all days in a leap year.
   (c) This means that the range of the function f is equal to its codomain.
2. (a) The domain of the function s is the set of natural numbers.
   (b) A codomain for the function s is the set of natural numbers.
   (c) This means that the range of s is not equal to the set o natural numbers.

Progress Check 6.3

1. $f(-1) \approx -3$ and $f(2) \approx -2.5$.
2. Values of x for which $f(x) = 2$ are approximately -2.8, -1.9, 0.3, 1.2, and 3.5.
3. The range of f appears to be the closed interval [-3.2, 3.2] or $\{y \in \mathbb{R} \mid -3.2 \leq y \leq 3.2\}$.

Progress Check 6.4

Only the arrow diagram in Figure (a) can be used to represent a function from A to B. The range of this function is the set $\{a, b\}$.

Section 6.2

Progress Check 6.5

1. $f(0) = 0$, $f(1) = 1$, $f(2) = 1$, $f(3) = 1$, $f(4) = 1$.
2. $g(0) = 0$, $g(1) = 1$, $g(2) = 2$, $g(3) = 3$, $g(4) = 4$.

Progress Check 6.6

$I_{\mathbb{Z}_5} \neq f$ and $I_{\mathbb{Z}_5} = g$

Progress Check 6.7

1. 3.5
2. 4.02
3. \(\dfrac{\pi + \sqrt{2}{4}\)
4. The process of finding the average of a finite set of real numbers can be thought of as a function from $\mathcal{F}(\mathbb{R})$ to $\mathbb{R}$. So the domain is $\mathcal{F}(\mathbb{R})$, the codomain is $\mathbb{R}$, and we can define a function avg: $\mathcal{F}(\mathbb{R}) \to \mathbb{R}$ as follows: If $A \in \mathcal{F}(\mathbb{R})$ and $A = \{a_1, a_2, ..., a_n\}$, then $\text{ave}(A) = \dfrac{a_1 + a_2 + \cdots a_n}{n}$.

Progress Check 6.8

1. The sixth terms is $\dfrac{1}{18}$ and the tenth term is $\dfrac{1}{30}$.
2. The sixth terms is $\dfrac{1}{36}$ and the tenth term is $\dfrac{1}{100}$.
3. The sixth terms is 1 and the tenth term is 1.

Progress Check 6.9

1. $g(0,3) = -3$; $g(3,-2) = 11$; $g(-3,-2) = 11$; $g(7,-1) = 50$.
2. $\{(m,n) \in \mathbb{Z} \times \mathbb{Z} \mid n = m^2\}$
3. $\{(m,n) \in \mathbb{Z} \times \mathbb{Z} \mid n = m^2 - 5\}$

Section 6.3

Progress Check 6.10

The functions k, F, and s are injections. The functions f and h are not injections.

Progress Check 6.11

The functions f and s are surjections. The functions k and F are not surjections.

Progress Check 6.15

The function f is an injection but not a surjection. To see that it is an injection, let $a, b \in \mathbb{R}$ and assume that $f(a) = f(b)$. This implies that $e^{-a} = e^{-b}$. Now use the natural logarithm function to prove that $a = b$. Since $e^{-x} > 0$ for each real number x, there is no $x \in \mathbb{R}$ such that $f(x) = -1$. So f is not a surjection.

The function g is an injection and is a surjection. The proof that g is an injection is basically the same as the proof that f is an injection. To prove that g is a surjection, let $b \in R_+$. To construct the real number a such that g.a/ D b, solve the equation $e^{-a} = b$ for a. The solution is $a = -\ln b$. It can then be verified that $g(a) = b$.

Progress Check 6.16

1. There are several ordered pairs $(a, b) \in \mathbb{R} \times \mathbb{R}$ such that $g(a,b) = 2$. For example, $g(0,2) = 2$, $g(-1,4) = 2$, and $g(2,-2) = 2$.
2. For each $z \in \mathbb{R}$, $g(0,z) = z$.
3. Part (1) implies that the function g is not an injection. Part (2) implies that the function g is a surjection since for each $z \in \mathbb{R}$, $(0,z)$ is in the domain of g and $g(0,z) = z$.

Section 6.4

Progress Check 6.17

The arrow diagram for $g \circ f : A \to B$ should show the following:

$$\begin{aligned} (g \circ f)(a) &= g(f(a)) & (g \circ f)(b) &= g(f(b)) \\ &= g(2) = 1 & &= g(3) = 2 \\ (g \circ f)(c) &= g(f(c)) & (g \circ f)(d) &= g(f(d)) \\ &= g(1) = 3 & &= g(2) = 1 \end{aligned}$$

The arrow diagram for $g \circ g : B \to B$ should show the following:

$$\begin{array}{rclrcl}
(g \circ f)(1) & = & g(g(1)) & (g \circ g)(2) & = & g(g(2)) \\
 & = & g(3) = 2 & & = & g(1) = 3 \\
(g \circ g)(3) & = & g(g(3)) & & & g(f(d)) \\
 & = & g(2) = 1 & & &
\end{array}$$

Progress Check 6.18

1. $F = g \circ f$, where $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 + 3$, and $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^3$.
2. $G = h \circ f$, where $f : \mathbb{R} \to \mathbb{R}^+$ by $f(x) = x^2 + 3$, and $h : \mathbb{R}^+ \to \mathbb{R}$ by $h(x) = \text{In}x$.
3. $f = g \circ k$, where $k : \mathbb{R} \to \mathbb{R}$ by $k(x) = x^2 - 3$, and $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = |x|$.
4. $g = h \circ f$, where $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = \dfrac{2x-3}{x^2+1}$, and $h : \mathbb{R} \to \mathbb{R}$ by $h(x) = \cos x$.

Progress Check 6.19

For the examples that are constructed:

1. $g \circ f$ should be an injection.
2. $g \circ f$ should be a surjection.
3. $g \circ f$ should be a bijection.

Section 6.5

Progress Check 6.23

Neither set can be used to define a function.

1. The set F does not satisfy the first condition of Theorem 6.22.
2. The set G does not satisfy the second condition of Theorem 6.22.

Progress Check 6.24

2. $f^{-1} = \{(r,a), (p,b), (q,c)\}$
$h^{-1} = \{(p,a), (q,b), (r,c), (q,d)\}$
$g^{-1} = \{(p,a), (q,b), (p,c)\}$

3. (a) f^{-1} is a function from C to A.
(b) g^{-1} is not a function from C to A since $(p,a) \in g^{-1}$ and $(p,c) \in g^{-1}$.
(c) h^{-1} is not a function from C to B since $(q,b) \in h^{-1}$ and $(q,d) \in h^{-1}$.

5. In order for the inverse of a function $F : S \to T$ to be a function from T to S, the function F must be a bijection.

Section 6.6

Progress Check 6.30

1. $f(A) = \{s,t\}$
2. $f(B) = \{f(x) \mid x \in b\} = \{x\}$
3. $f^{-1}(C) = \{x \in S \mid f(x) \in C\} = \{a,b,c,d\}$
4. $f^{-1}(D) = \{x \in S \mid f(x) \in D\} = \{a,d\}$

Progress Check 6.32

1. $f(0) = 2$ $f(2) = 6$ $f(4) = 2$ $f(6) = 6$
   $f(1) = 3$ $f(3) = 3$ $f(5) = 3$ $f(7) = 3$
2. (a) $f(A) = \{2,3,6\}$ $f^{-1}(C) = \{0,1,3,4,5,7\}$
   $f(B) = \{2,3,6\}$ $f^{-1}(D) = \{1,3,5,7\}$
3. (a) $f(A) \cap f(B) = \{2\}$ $f(A) \cap f(B) = \{2,3,6\}$
   So in this case, $f(A \cap B) \subseteq f(A) \cap f(B)$.
   (b) $f(A) \cup f(B) = \{2,3,6\}$ $f(A \cup B) = \{2,3,6\}$
   So in this case, $f(A \cap B) \subseteq f(A \cup B)$.
   (c) $f^{-1}(C) \cap f^{-1}(D) = f^{-1}(C \cap D) = \{1,3,5,7\}$. So in this case, $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.
   (d) $f^{-1}(C) \cup f^{-1}(D) = f^{-1}(C \cup D) = \{0,1,3,4,5,7\}$. So in this case, $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.
4. $f(A) = \{2,3,6\}$. Hence, $f^{-1}(f(A)) = \{0,1,2,3,4,5,6,7\}$. So in this case, $A \subseteq f^{-1}(f(A))$.

Section 7.1

Progress Check 7.2

1. (a) T is a relation on $\mathbb{R}$ since S is a subset of $\mathbb{R} \times \mathbb{R}$.
   (b) Solve the equation $x^2 + 4^2 = 64$. This gives $x = \pm\sqrt{48}$.
   Solve the equation $x^2 + 9^2 = 64$. There are no real number solutions. So there does not exist an $x \in \mathbb{R}$ such that $(x, 9) \in S$.
   (c) dom$(T) = \{x \in \mathbb{R} \mid -8 \leq x \leq 8\}$ range$(T) = \{y \in \mathbb{R} \mid -8 \leq y \leq 8\}$
   (d) The graph is a circle of radius 8 whose center is at the origin.
2. (a) R is a relation on A since R is a subset of $A \times A$.
   (b) If we assume that each state except Hawaii has a land border in common with itself, then the domain and range of R are the set of all states except Hawaii. If we do not make this assumption, then the domain and range are the set of all states except Hawaii and Alaska.
   (c) The first statement is true. If x has a land border with y, then y has a land border with x. The second statement is false. Following is a counterexample: (Michigan, Indiana) $\in R$, (Indiana, Illinois) $\in R$, but (Michigan, Illinois) $\notin R$.

Progress Check 7.3

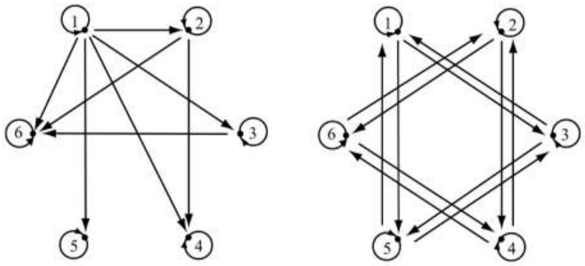
1. The domain of the divides relation is the set of all nonzero integers. The range of the divides relation is the set of all integers.
2. (a) This statement is true since for each $a \in \mathbb{Z}$, $a = a \cdot 1$.
   (b) This statement is false: For example, 2 divides 4 but 4 does not divide 2.
   (c) This statement is true by Theorem 3.1 on page 88.

Progress Check 7.4

1. Each element in the set F is an ordered pair of the form (x, y) where $y = x^2$.
2. (a) $A = \{-2, 2\}$
   (b) $B = \{-\sqrt{10}, \sqrt{10}\}$
   (c) $C = \{25\}$
   (d) $D = \{9\}$
3. The graph of $y = x^2$ is a parabola with vertex at the origin that is concave up.

Progress Check 7.5

The directed graph for Part (a) is on the left and the directed graph for Part (b) is on the right.



Section 7.2

Progress Check 7.7

The relation R:

- Is not reflexive since $(c, c) \notin R$ and $(d, d) \notin R$.
- Is symmetric.
- Is not transitive. For example, $(c, a) \in R$, $(a, c) \in R$, but $(c, c) \notin R$.

Progress Check 7.9

- Proof that the relation $\sim$ is symmetric: Let $a, b \in \mathbb{Q}$ and assume that $a \sim b$. This means that $a - b \in \mathbb{Z}$. Therefore, $-(a - b) \in \mathbb{Z}$ and this means that $b - a \in \mathbb{Z}$, and hence, $b \sim a$.

- Proof that the relation $\sim$ is transitive: Let $a, b, c \in \mathbb{Q}$and assume that $a \sim b$ and $b \sim c$. This means that $a - b \in \mathbb{Z}$ and that $b - c \in \mathbb{Z}$. Therefore, $((a - b) + (b - c)) \in \mathbb{Z}$ and this means that $a - c \in \mathbb{Z}$, and hence, $a \sim c$.

Progress Check 7.11

The relation $\approx$ is reflexive on $\mathcal{P}(U)$ since for all $A \in \mathcal{P}(U)$, card(A)= card(A).

The relation $\approx$ is symmetric since for all $A, B \in \mathcal{P}(U)$, if card(A) = card(B), then using the fact that equality on $\mathbb{Z}$ is symmetric, we conclude that card(B) = card(A). That is, if A has the same number of elements as B, then B has the same number of elements as A.

The relation $\approx$ is transitive since for all $A, B, C \in \mathcal{P}(U)$, if card($A$) = card($B$) and card($B$) = card($C$), then using the fact that equality on $\mathbb{Z}$ is transitive, we conclude that card(A) = card(C). That is, if A and B have the same number of elements and B and C have the same number of elements, then A and C have the same number of elements.

Therefore, the relation $\approx$ is an equivalence relation on $\mathcal{P}(U)$.

Section 7.3

Progress Check 7.12

The distinct equivalence classes for the relation R are: $\{a, b, e\}$ and $\{c, d\}$.

Progress Check 7.13

The distinct congruence classes for congruence modulo 4 are

[0] = {..., -12, -8, -4, 0, 4, 8, 12, ...} [1] = {..., -11, -7, -3, 1, 5, 9, 13, ...}
[2] = {..., -10, -6, -2, 2, 6, 10, 14, ...} [1] = {..., -9, -5, -1, 3, 7, 11, 15, ...}

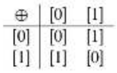
Progress Check 7.15

1. [5] = [-5] = {-5, 5} [π] = [-π] = {-π, π}
   [10] = [-10] = {-10, 10}
2. [0] = {0}
3. [a] = {-a, a}

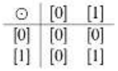
Section 7.4

Progress Check 7.2

1.

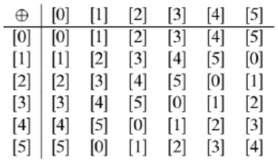


⊕	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

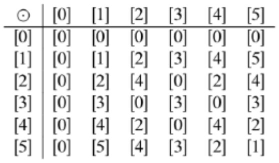


⊙	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

2.



⊕	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]



⊙	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

3. For all $a, b \in \mathbb{Z}$, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.
4. The statement in (a) is true and the statement in (b) is false. For example, in $\mathbb{Z}_6$, $[2] \odot [3] = [0]$.

Section 8.1

Progress Check 8.2

1. The remainder is 8.
2. gcd(12, 8) = 4
3. $12 = 8 \cdot 1 + 4$ and gcd(r, r_2) = gcd(8, 4) = 4.

Progress Check 8.4

1.

Original Pair	Equation from Division Algorithm	New Pair
(180, 126)	$180 = 126 \cdot 1 + 54$	(126, 54)

(126, 54)	$126 = 54 \cdot 2 + 18$	(54, 18)
(54, 18)	$54 = 18 \cdot 3 + 0$	

Consequently, gcd(180, 126) = 18.

2.

Original Pair	Equation from Division Algorithm	New Pair
(4208, 288)	$4208 = 288 \cdot 14 + 176$	(288, 176)
(288, 176)	$288 = 126 \cdot 1 + 112$	(176, 112)
(176, 112)	$176 = 112 \cdot 1 + 64$	(112, 64)
(112, 64)	$112 = 64 \cdot 1 + 48$	(64, 48)
(64, 48)	$64 = 48 \cdot 1 + 16$	(48, 16)
(48, 16)	$48 = 16 \cdot 3 + 0$	

Consequently, gcd(4208. 288) = 16.

Progress Check 8.7

1. From Progress Check 8.4, gcd(180, 126) = 18.

$$\begin{aligned} 18 &= 126 - 54 \cdot 2 \\ &= 126 - (180 - 126) \cdot 2 \\ &= 126 \cdot 3 + 180 \cdot (-2) \end{aligned} \tag{Appendix B.18}$$

   So gcd(180, 126) = 18, and $18 = 126 \cdot 3 + 180 \cdot (-2)$.
2. From Progress Check 8.4, gcd(4208. 288) = 16.

$$\begin{aligned} 16 &= 64 - 48 \\ &= 64 - (112 - 64) = 64 \cdot 2 - 112 \\ &= (176 - 112) \cdot 2 - 112 = 176 \cdot 2 - 112 \cdot 3 \quad = \begin{array}{l} 176 \cdot 2 - (288 - 176) \cdot 3 \\ = 176 \cdot 5 - 288 \cdot 3 \end{array} \\ &= (4208 - 288 \cdot 14) \cdot 5 - 288 \cdot 3 \\ &= 4208 \cdot 5 + 288 \cdot (-73) \end{aligned} \tag{Appendix B.19}$$

   So gcd(4208. 288) = 16, and $16 = 4208 \cdot 5 + 288 \cdot (-73)$.

Section 8.2

Progress Check 8.10

1. If $a, p \in \mathbb{Z}$, p is prime, and p divides a, then gcd(a, p) = p.
2. If $a, p \in \mathbb{Z}$, p is prime, and p does not divide a, then gcd(a, p) = 1.
3. Three examples are gcd(4, 9) = 1, gcd(15, 16) = 1, gcd(8, 25) = 1.

Progress Check 8.13

Theorem 8.12. Let a, b, and c be integers. If a and b are relatively prime and $a \mid (bc)$. We will prove that a divides c.

Proof. Let a, b, and c be integers. Assume that a and b are relatively prime and $a \mid (bc)$. We will prove that a divides c.

Since a divides bc, there exists an integer k such that

$$bc = ak. \tag{Appendix B.20}$$

In addition, we are assuming that a and b are relatively prime and hence gcd(a, b) = 1. So by Theorem 8.9, there exist integers m and n such that

$$am + bn = 1. \tag{Appendix B.21}$$

We now multiply both sides of equation (B.21) by c. This gives

$$\begin{aligned} (am + bn)c &= 1 \cdot c \\ acm + bcn &= c \end{aligned} \tag{Appendix B.22}$$

We can now use equation (B.20) to substitute $bc = ak$ in equation (B.22) and obtain

$$acm + akn = c.$$

If we now factor the left side of this last equation, we see that $a(cm + kn) = c$. Since $(cm + kn)$ is an integer, this proves that a divides c. Hence, we have proven that if a and b are relatively prime and $a \mid (bc)$, then $a \mid c$.

Section 8.3

Progress Check 8.20

2. $x = 2 + 3k$ and $y = 0 - 2k$, where k can be any integer. Again, this does not prove that these are the only solutions.

Progress Check 8.21

One of the Diophantine equations in Preview Activity 2 was $3x + 5y = 11$. We were able to write the solutions of this Diophantine equation in the form

$$x = 2 + 5k \text{ and } y = 1 - 3k,$$

where k is an integer. Notice that $x = 2$ and $y = 1$ is a solution of this equation. If we consider this equation to be in the form $ax + by = c$, then we see that $a = 3$, $b = 5$, and $c = 11$. Solutions for this equation can be written in the form

$$x = 2 + bk \text{ and } y = 1 - ak,$$

where k is an integer.

The other equation was $4x + 6y = 16$. So in this case, $a = 4$, $b = 6$, and $c = 16$. Also notice that $d = \gcd(4, 6) = 2$. We note that $x = 4$ and $y = 0$ is one solution of this Diophantine equation and solutions can be written in the form

$$x = 4 + 3k \text{ and } y = 0 - 2k,$$

where k is an integer. Using the values of a, b, and d given above, we see that the solutions can be written in the form

$$x = 2 + \frac{b}{d}k \text{ and } y = 0 - \frac{a}{d},$$

where k is an integer.

Progress Check 8.24

1. Since 21 does not divide 40, Theorem 8.22 tells us that the Diophantine equation $63x + 336y = 40$ has no solutions. Remember that this means there is no ordered pair of integers (x, y) such that $63x + 336y = 40$. However, if we allow x and y to be real numbers, then there are real number solutions. In fact, we can graph the straight line whose equation is $63x + 336y = 40$ in the Cartesian plane. From the fact that there is no pair of integers x, y such that $63x + 336y = 40$, we can conclude that there is no point on the graph of this line in which both coordinates are integers.
2. To write formulas that will generate all the solutions, we first need to find one solution for $144x + 225y = 27$. This can sometimes be done by trial and error, but there is a systematic way to find a solution. The first step is to use the Euclidean Algorithm in reverse to write gcd(144, 225) as a linear combination of 144 and 225. See Section 8.1 to review how to do this. The result from using the Euclidean Algorithm in reverse for this situation is

   $$144 \cdot 11 + 225 \cdot (-7) = 9. \tag{Appendix B.23}$$

   If we multiply both sides of this equation by 3, we obtain

   $$144 \cdot 33 + 225 \cdot (-21) = 27. \tag{Appendix B.24}$$

   This means that $x_0 = 33$, $y_0 = -21$ is a solution of the linear Diophantine equation $144x + 225y = 27$. We can now use Theorem 8.22 to conclude that all solutions of this Diophantine equation can be written in the form

$$x = 33 + \frac{225}{9}k \qquad y = -21 - \frac{144}{9}k, \tag{Appendix B.25}$$

where $k \in \mathbb{Z}$.
We check this general solution as follows: Let $k \in \mathbb{Z}$. Then

$$\begin{aligned} 144x + 225y &= 144(33 + 25k) + 225(-21 - 16k) \\ &= (4752 + 3600k) + (-4725 - 3600k) \\ &= 27. \end{aligned} \tag{Appendix B.26}$$

Section 9.1

Progress Check 9.2

1. We first prove that $f : A \to B$ is an injection. So let $x, y \in A$ and assume that $f(x) = f(y)$. Then $x + 350 = y + 350$ and we can conclude that $x = y$. Hence, f is an injection. To prove that f is a surjection, let $b \in B$. Then $351 \le b \le 450$ and hence, $1 \le b - 350 \le 100$ and so $b - 350 \in A$. In addtion, $f(b - 350) = (b - 350) + 350 = b$. This proves that f is a surjection, Hence, the function f is a bijection, and so, $A \approx B$.
2. If x and t are even integers and $F(x) = F(t)$, then $x + 1 = t + 1$ and, hence, $x = t$. Therefore, F is an injection.
   To prove that F is a surjection, let $y \in D$. This means that y is an odd integer and, hence, $y - 1$ is an even integer. In addition,

   $$F(y - 1) = (y - 1 + 1 = y. \tag{Appendix B.27}$$

   Therefore, F is a surjection and hence, F is a bijection. We conclude that $E \approx D$.
3. Let $x, t \in (0, 1)$ and assume that $f(x) = f(t)$. Then $bx = bt$ and, thence, $x = t$. Therefore, f is an injection.
   To prove that f is a surjection, let $y \in (0, b)$. Since $0 < y < b$, we conclude that $0 < \frac{y}{b} < 1$ and that

   $$f(\frac{y}{b}) - b(\frac{y}{b}\backslash) = y. \tag{Appendix B.28}$$

   Therefore, f is a surjection and hence f is a bijection. Thus, $(0, 1) \approx (0, b)$.

Section 9.2

Progress Check 9.11

1. The set of natural numbers $\mathbb{N}$ is a subset of $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$. Since $\mathbb{N}$ is an infinite set, we can use Part (2) of Theorem 9.10 to conclude that $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are infinite sets.
2. Use Part (1) of Theorem 9.10.
3. Prove that $\mathbb{E}^+ \approx \mathbb{N}$ and use Part (1) of Theorem 9.10.

Progress Check 9.12

1. Use the definition of a countably infinite set.
2. Since $\mathbb{E}^+ \approx \mathbb{N}$, we can conclude that card$(E^+) = \aleph_0$.
3. One function that can be used is $f : S \to \mathbb{N}$ defined by $f(m) = \sqrt{m}$ for all $m \in S$.

Progress Check 9.23

Player Two has a winning strategy. On the kth turn, whatever symbol Player One puts in the kth position of the kth row, Player Two must put the other symbol in the kth position of his or her row. This guarantees that the row of symbols produced by Player Two will be different that any of the rows produced by Player One.

This is the same idea used in Cantor's Diagonal Argument. Once we have a "list" of real numbers in normalized form, we create a real number that is not in the list by making sure that its kth decimal place is different than the kth decimal place for the kth number in the list. The one complication is that we must make sure that our new real number does not have a decimal expression that ends in all 9's. This was done by using only 3's and 5's.

Progress Check 9.25

1. ***Proof***. In order to find a bijection $f:(0,1)\rightarrow(a,b)$, we will use the linear function through the points $(0,a)$ and $(1,b)$. The slope is $(b-a)$ and the y-intercept is $(0,a)$. So define $f:(0,1)\rightarrow(a,b)$ by

   $$f(x)=(b-a)x+a, \text{ for each } x\in(0,1). \tag{Appendix B.29}$$

   Now, if $x,t\in(0,1)$ and $f(x)=f(t)$, then

   $$(b-a)x+a=(b-a)t+a. \tag{Appendix B.30}$$

   This implies that $(b-a)x=(b-a)t$, and since $b-a\neq 0$, e can conclude that $x=t$. Therefore, f is an injection.
   To prove that f is a surjection, we let $y\in(a,b)$. If $x=\dfrac{y-a}{b-a}$, then

   Missing argument for \begin

   This proves that f is a surjection. Hence, f is a bijection and $(0,1)\approx(a,b)$. Therefore, (a,b) is uncountable and has cardinality c.
2. Now, if a,b,c,d are real number with $a<b$ and $c<d$, then we know that

   $$(a,b)\approx(0,1) \text{ and } (c,d)\approx(0,1). \tag{Appendix B.31}$$

   Since ≈ is an equivalence relation, we can conclude that $(a,b)\approx(c,d)$.

Appendix C: Answers and Hints for Selected Exercises

Section 1.1

1. Sentences (a), (c),(e), (f), (j) and (k) are statements. Sentence (h) is a statement if we are assuming that n is a prime number means that n is an integer.
2.

	Hypothesis	Conclusion
a.	n is a prime number.	n^2 has three positive divisors.
b.	a is an irrational number and b is an irrational number.	$a \cdot b$ is an irrational number.
c.	p is a prime number.	$p = 2$ or p is an odd number.
d.	p is a prime number and $p \neq 2$.	p is an odd number.

3. Statements (a), (c), and (d) are true.
4. (a) True when $a \neq 3$. (b) True when $a = 3$.

6. (a) This function has a maximum value when $x = \frac{5}{16}$.
(c) No conclusion can be made about this function.

9. (a) The set of rational numbers is not closed under division.
(b) The set of rational number sis not closed undre division since division by zero is not defined.
(c) The set of nonzero rational numbers is closed under division.
(d) The set of positive rational numbers is closed under division.
(e) The set of positive real numbers is not closed under subtraction.
(f)The set of negative rational numbers is not closed under division.
(g)The set of negative integers is closed under addition.

Section 1.2

1. (a)

Step	Know	Reason
P	m is an even integer.	Hypothesis
$P1$	There exists an integers k such that $m = 2k$.	Definition of an even integer
$P2$	$m + 1 = 2k + 1$	Algebra
$Q1$	There exists an integer q such that $m + 1 = 2q + 1$.	Substitution of $k = q$
Q	$m + 1$ is an odd integer.	Definition of an odd integer

2. (c) We assume that x and y are odd integers and will prove that $x + y$ is an even integer. Since x and y are odd, there exist integers m and n such that $x = 2m + 1$ and $y = 2n + 1$. Then

$$\begin{aligned} x + y &= (2m+1) + (2n+1) \\ &= 2m + 2n + 2 \\ &= 2(m+n+1). \end{aligned} \tag{Appendix C.1}$$

Since the integers are closed under addition, $(m + n + 1)$ is an integer, and hence the last equation shows that $x + y$ is even. Therefore, we have proven that if x and y are odd integers, then $x + y$ is an even integer.
3. (b) Use Part (a) to prove this.

6. (a) Prove that their difference is equal to zero or prove that they are not zero and their quotient is equal to 1.
(d) Provethattwoofthesideshavethesamelength.Provethatthetriangle has two congruent angles. Prove that an altitude of the triangle is a perpendicular bisector of a side of the triangle.

9. (a) Some examples of type 1 integers are -5, -2, 1, 4, 7, 10.
(c) All example should indicate the proposition is true.

10. (a) Let a and b be integers and assume that a and b are both type 1 integers. Then, there exist integers m and n such that $a = 3m + 1$ and $b = 3n + 1$. Now show that

$$a + b = 3(m + n) + 2.$$

The closure properties of the integers imply that $m + n$ is an integer. Therefore, the last equation tells us that $a + b$ is a type 2 integer. Hence, we have proved that if a and b are both type 1 integers, then $a + b$ is a type 2 integer.

Section 2.1

1. The statement was true. When the hypothesis is false, the conditional statement is true.

2. (a) P is false .
(b) $P \wedge Q$ is false.
(c) $P \vee Q$ is false.

4. (c) Cannot tell if $P \wedge R$ is true or false.

5. Statements (a) and (d) have the same truth table. Statements (b) and (c) have the same truth tables.

7. The two statements have the same truth table.

9. (c) The integer x is even only if x^2 is even.
(d) The integer x^2 is even is necessary for x to be even.

Section 2.2

1. (a) Converse: If $a^2 = 25$, then $a = 5$. Contrapositive: If $a^2 \neq 25$, then $a \neq 5$.
(b) Converse: If Laura is playing golf, then it is not raining. Contrapositive: If Laura is not playing golf, then it is raining.

2. (a) Disjunction: $a \neq 5$ or $a^2 = 25$. Negation: $a = 5$ and $a^2 = 25$.
(b) Disjunction: It is raining or Laura is playing golf. Negation: It is not raining and Laura is not playing golf.

3. (a) We will not win the first game or we will not win the second game.
(c) You mow the lawn and I will not pay you \$20.
(f) You graduate from college, and you will not get a job and you will not go to graduate school.

7. (a) In this case, it may be better to work with the right side first.

$$\begin{aligned}
(P \to R) \vee (Q \to R) &\equiv (\urcorner R \vee R) \vee (\urcorner Q \vee R) \\
&\equiv (\urcorner R \vee \urcorner Q) \vee (R \vee R) \\
&\equiv (\urcorner R \vee \urcorner Q) \vee R \qquad \equiv \urcorner(P \vee Q) \vee R \\
&\equiv (P \wedge Q) \to R.
\end{aligned}$$

10. Statements (c) and (d) are logically equivalent to the given conditional statement. Statement (f) is the negation of the given conditional statement.
11. (d) This is the contrapositive of the given statement and hence, it is logically equivalent to the given statement.

Section 2.3

1. (a) $\frac{1}{2}, -2\}$
(d) $\{1, 2, 3, 4\}|$
(e) $\{0.5, 4.5\}$

2. $A = \{n^2 \mid n \in \mathbb{N}$
$D = \{4n \mid n\text{is a nonnegative integer and } 0 \leq n \leq 25\}$

3. The sets in (b) and (c) are equal to the given set.

5. (a) $\{x \in \mathbb{Z} \mid x \leq 5\}$
(e) \(\{x \in \mathbb{R}\ |\ x^2 > 10\}\)

Section 2.4

1. (a) There exists a rational number x such that $x^2 - 3x - 7 = 0$. This statement is false since the solutions of the equation are $x = \dfrac{3 \pm \sqrt{37}}{2}$, which are irrational numbers.

2. (b) $x = 0$ is a counterexample. The negation is: There exists a real number x such that $x^2 \leq 0$.
(g) $x = \dfrac{\pi}{2}$ is a counterexample. The negation is: There exists a real number x such that $\tan^2 x + 1 \neq \sec^2 x$.

3. (a) There exists a rational number x such that $x > \sqrt{2}$.
The negation is $(\forall x \in \mathbb{Q})(x \leq \sqrt{2})$, which is, For each rational number x, $x \leq \sqrt{2}$.

(c) For each integer x, x is even or x is odd.
The negation is ($\exists x \in \mathbb{Z}$ (x is odd and x is even), which is, There exists an integer x such that x is odd and x is even.

(e) For each integer x, if x^2 is odd, then x is odd.
The negation is ($\exists x \in \mathbb{Z}$ (x^2 is odd and x is even), which is, There exists an integer x such that x^2 is odd and x is even.
(h) There exists a real number x such that cos(2x) = 2 (cos$x$).
The negation is ($\forall x \in \mathbb{R}$ (cos(2x) $\neq$ 2(cos$x$)), which is, For each real number x, cos(2x) $\neq$ 2(cos$x$).

4. (a) There exist integers m and n such that $m > n$.
(c) There exists an integer n such that for each ineger m, $m^2 > n$.

5. (a) $(\forall m)(\forall n)(m \leq n)$.
For all inetgers m and n, $m \leq n$.
(e) $(\forall n)(\exists m)(m^2 \leq n)$.
For each integer n, there exists an integer m such that $m^2 \leq n$.

10. (a) A function f with domain $\mathbb{R}$ is strictly increasing provided that $(\forall x, y \in \mathbb{R})[(x < y) \rightarrow (f(x) < f(y))]$.

Section 3.1

1. (a) Remember that to prove that $a \mid (b - c)$, you need to prove that there exists an integer q such that $b - c = a \cdot q$.
(b) What do you need to do in order to prove that n^3 is odd? Notice that ifn is an odd integer, then there exists an integer k such that $n = 2k + 1$. Remember that to prove that n^3 is an odd integer, you need to prove that there exists an integer q such that $n^3 = 2q + 1$.
Or you can approach this as follows: If n is odd, then by Theorem 1.8, n^2 is odd. Now use the fact that $n^3 = n \cdot n^2$.
(c) If 4 divides $(a - 1)$, then there exists an integer k such that $a - 1 = 4k$. Write $a = 4k + 1$ and then use algebra to rewrite $(a^2 - 1)$.

3. (e) Make sure you first try some examples. How do you prove that an integer is an odd integer?
(f) The following algebra may be useful.

$$4(2m+1)^2 + 7(2m+1) + 6 = 6m^2 + 30m + 17.$$

4. (a) If $xy = 1$, then x and y are both divisors of 1, and the only divisors of 1 are -1 and 1.|
(b) Part (a) is useful in proving this.

3. Let $n \in \mathbb{N}$. For $a, b \in \mathbb{Z}$, you need to prove that if $a \equiv b$ (mod n), then $b \equiv a$ (mod n). Remember that for $x, y \in \mathbb{Z}$, $x \equiv y$ (mod n) if and only if $n \mid (x - y)$.

5. **Another hint**: $(4n + 3) - 2(2n + 1) = 1$.

8. (a) Assuming a and b are both congruent to 2 modulo 3, there exist integers m and n such that $a = 3m + 2$ and $b = 3n + 2$. Then show that

$$a + b = 3(m + n + 1) + 1$$

12. The assumptions mean that $n \mid (a - b)$ and that $n \mid (c - d)$. Use these divisibility relations to obtain an expression that is equal to a and to obtain an expression that is equal to c. Then use algebra to rewrite the resulting expressions for $a + c$ and $a \cdot c$.

Section 3.2

1. (a) Let n be an even integer. Since n is even, there exists an integer k such that $n = 2k$. Now use this to prove that n^3 must be even.
(b) Prove the contrapositive.
(c) Explain why Parts (a) and (b) prove this.
(d) Explain why Parts (a) and (b) prove this.

2. (a) The contrapositive is, For all integers a and b, if $ab \equiv 0$ (mod 6), then $a \equiv 0$ (mod 6) or $b \equiv 0$ (mod 6).

4. (a) If $a \equiv 2$ (mod 5), then there exists an integer k such that $a - 2 = 5k$. Then $a^2 = (2 + 5k)^2 = 4 + 20k + 25k^2$. This means that $a^2 - 4 = 5(4k + 5k^2)$.

6. One of the two conditional statements is true and one is false.

8. Prove both of the conditional statements: (1) If the area of the right triangle is $c^2/4$, then the right triangle is an isosceles triangle. (2) If the right triangle is an isosceles triange, then the area of the right triangle is $c^2/4$.

9. Prove the contrapositive.

10. Remember that there are two conditional statements associated with this biconditional statement. Be willing to consider the contrapositive of one of these conditional statements.

15. Define an appropriate function and use the Intermediate Value Theorem.

17. (b) Since 4 divides a, there exist an integer n such that $a = 4n$. Using this, we see that $b^3 = 16n^2$. This means that b3 is even and hence by Exercise (1), b is even. So there exists an integer m such that $b = 2m$. Use this to prove that m^3 must be even and hence by Exercise (1), m is even.

18. It may be necessary to factor a sum cubes. Recall that

$$u^3 + v^3 = (u + v)(u^2 - uv + v^2).$$

Section 3.3

1. (a) $P \vee C$

3. (a) Let r be a real number such that $r^2 = 18$. We will prove that r is irrational using a proof by contradiction. So we assume that r is a rational number.
(b) Do not attempt to mimic the proof that the square root of 2 is irrational (Theorem 3.20). You should still use the definition of a rational number but then use the fact that $\sqrt{18} = \sqrt{9 \cdot 2} = \sqrt{9}\sqrt{2} = 3\sqrt{2}$.

5. In each part, what is the contrapositive of the proposition? Why does it seem like the contrapositive will not be a good approach? For each statement, try a proof by contradiction.

6. Two of the propositions are true and the other two are false.

11. Recall that $\log_2 32$ is the real number a such that $2^a = 32$. That is, $a = \log_2 32$ means that $2^a = 32$. If we assume that a is rational, then there exist integers m and n, with $n \neq 0$, such that $a = \dfrac{m}{n}$.

12. **Hint:** The only factors of 7 are -1, 1, -7, and 7.

13. (a) What happens if you expand $(\sin\theta + \cos\theta)^2$? Don'tforgetyourtrigono- metric identities.

14. **Hint**: Three consecutive natural numbers can be represented by n, $n + 1$, and $n + 2$, where $n \in \mathbb{N}$, or three consecutive natural numbers can be represented by $m - 1$, m and $m + 1$, where $m \in \mathbb{N}$.

Section 3.4

1. Use the fact that $n^2 + n = n(n + 1)$.

2. Do not use the quadratic formula. Try a proof by contradiction. **Hint**: If there exists a solution of the equation that is an integer, then we can conclude that there exists an integer n such that $n^2 + n - u = 0$.

3. First write $n = 2m + 1$ for some integer m. The integer m can be even or odd.

5. (c) For all integers a, b, and d with $d \neq 0$, if d divides the product ab, then d divides a or d divdes b.

8. Try a proof by contradiction with two cases: a is even or a is odd.

10. (a) One way is to use three cases: (i) $x > 0$; (ii) $x = 0$; and $x < 0$. For the first case, $-x < 0$ and $|-x| = -(-x) = x = |x|$.

11. (a) For each real number x, $|x| \geq a$ if and only if $x \geq a$ or $x \leq -a$.

Section 3.5

2. (b) Factor $n^3 - n$.
(c) Consider using cases based on congruence modulo 6.

3. Let $n \in \mathbb{N}$. For $a, b \in \mathbb{Z}$, you need to prove that if $a \equiv b$ (mod n), then $b \equiv a$ (mod n). Remember that for $a, b \in \mathbb{Z}$, if $a \equiv b$ (mod n), then $n \mid (a-b)$. So there exists an integer k such that $a - b = nk$.

4. (a) Use the definition of congruence.
(b) Let $a \in \mathbb{Z}$. Corollary 3.32 tell us that if $a \not\equiv 0$ (mod 3), then $a \equiv 1$ (mod 3) or $a \equiv 2$ (mod 3).
(c) For one of the conditional statements, Part (b) tells us we can use a proof by cases using the following two cases: (1) $a \equiv 1$ (mod 3); (2) $a \equiv 2$ (mod 3).

6. The result in Part (c) of Exercise (4) may be helpful in a proof by contradiction.

8. (a) Remember that $3 \mid k$ if and only if $k \equiv 0$ (mod 3).

9. (a) Use a proof similar to the proof of Theorem 3.20. The result of Exercise (8) may be helpful.

12. (a) Use the results in Theorem 3.28 to prove that the remainder must be 1.

Section 4.1

1. The sets in Parts (a) and (b) are inductive.

2. A finite nonempty set is not inductive (why?) but the empty set is inductive (why?).

3. (a) For each $n \in \mathbb{N}$, let $P(n)$ be, $2 + 5 + 8 + \cdots + (3n-1) = \dfrac{n(3n+1)}{2}$. Verify that $P(1)$ is true. The key to the inductive step is that if $P(k)$ is true, then

$$\begin{aligned} 2 + 5 + 8 + \cdots + (3k-1) + [3(k+1) - 1] &= (2 + 5 + 8 + \cdots + (3k-1)) + (3k+2) \\ &= \frac{3k(k+1)}{2} + (3k+2). \end{aligned}$$

Now use algebra to show that the last expression can be rewritten as $\dfrac{(k+1)(3k+4)}{2}$ and then explain why this completes the proof that if $P(k)$ is true, then $P(k+1)$ is true.

6. The conjecture is that for each $n \in \mathbb{N}$, $\sum_{j=1}^{n}(2j-1) = n^2$. The key to the inductive step is that

$$\begin{aligned} \textstyle\sum_{j=1}^{k+1}(2j-1) &= \textstyle\sum_{j=1}^{k}(2j-1) + [2(k+1) - 1] \\ &= \textstyle\sum_{j=1}^{k}(2j-1) + [2k+1]. \end{aligned}$$

8. (a) The key to the inductive step is that if $4^k = 1 + 3m$, then $4^k \cdot 4 = 4(1+3m)$, which implies that

$$4^{k+1} - 1 = 3(1 + 4m).$$

13. Let k be a natural number. If $a^k \equiv b^k$ (mod n), then since we are also assuming that $a \equiv b$ (mod n), we can use Part (2) of Theorem 3 to conclude that $a \cdot a^k \equiv b \cdot b^k$ (mod n).

14. Three consecutive natural numbers maybe represent by n, $n+1$, and $n+2$, where n is a natural number. For the inductive step, think before you try to do a lot of algebra. You should be able to complete a proof of the inductive step by expanding the cube of only one expression.

Section 4.2

1. (a) If $P(k)$ is true, then $3^k > 1 + 2^k$. Multiplying both sides of this inequality by 3 gives

$$3^{k+1} > 3 + 3 \cdot 2^k$$

Now, since $3 > 1$ and $3 \cdot 2^k > 2^{k+1}$, we see that $3 + 3 \cdot 2^k > 1 + 2^{k+1}$ and hence, $3^{k+1} > 1 + 2^{k+1}$. Thus, if $P(k)$ is ture, then $P(k+1)$ is true.

2. If $n \geq 5$, then $n^2 < 2^n$. For the inductive step, we assume that $k^2 < 2^k$ and that $k \geq 5$. With these assumptions, prove that

$$(k+1)^2 = k^2 + 2k + 1 < 2^k + 2k + 1.$$

Now use the assumption that $k > 4$ to prove that $2k + 1 < k^2$ and combine this with the assumption that $k^2 < 2^k$.

5. Let $P(n)$ be the predicate, "$8^n \mid (4n)!$." Verify that $P(0)$, $P(1)$, $P(2)$, and $P(3)$ are true. For the inductive step, the following fact about factorials may be useful:

$$\begin{aligned}[4(k+1)]! &= (4k+4)! \\ &= (4k+4)(4k+3)(4k+2)(4k+1)(4k)!.\end{aligned}$$

8. Let $P(n)$ be, "The natural number n can be written as a sum of natural numbers, each of which is a 2 or a 3." Verify that $P(4)$, $P(5)$, $P(6)$, and $P(7)$ are true.

To use the Second Principle of Mathematical Induction, assume that $k \in \mathbb{N}$, $k \geq 5$ and that $P(4)$, $P(5)$, ... $P(k)$ are true. Then notice that

$k + 1 = (k-1) + 2.$

Since $k - 1 \leq 4$, we have assume that $P(k-1)$ is true. Use this to complete the inductive step.

12. Let $P(n)$ be, “Any set with n elements has $\dfrac{n(n-1)}{2}$ 2-element subsets.” $P(1)$ is true since any set with only one element has no 2-element subsets. Let $k \in \mathbb{N}$ and assume that $P(k)$ is true. This means that any set with k elements has $\dfrac{k(k-1)}{2}$ 2-element subsets. Let A be a set with $k+1$ elements, and let $x \in A$. Now use the inductive hypothesis on the set $A - \{x\}$, and determine how the 2-element subsets of A are related to the set $A - \{x\}$.

16. (a) Use Theorem 4.9
(b) Assume $k \neq q$ and consider two cases: (i) $k < q$; (ii) $k > q$.

Section 4.3

1. For the inductive step, if $a_k = k!$, then

$$\begin{aligned}a_{k+1} &= (k+1)a_k \\ &= (k+1)k! \\ &= (k+1)!.\end{aligned}$$

2. (a) Let $P(n)$ be, " f_{4n} is a multiple of 3." Since $f_4 = 3$, $P(1)$ is true. If $P(k)$ is true, then there exists an integer m such that $f_{4k} = 3m$. Use the following:

$$\begin{aligned}f_{4(k+1)} &= f_{4k+4} \\ &= f_{4k+3} + f_{4k+2} \\ &= (f_{4k+2} + f_{4k+1}) + (f_{4k+1} + f_{4k}) \\ &= f_{4k+2} + 2f_{4k+1} + f_{4k} \\ &= (f_{4k+1} + f_{4k}) + 2f_{4k+1} + f_{4k}.\end{aligned}$$

(c) Let $P(n)$ be, "$f_1 + f_2 + \cdots + f_{n-1} = f_{n+1} - 1$." Since $f_1 = f_3 - 1$, $P(2)$ is true. For $k \geq 2$, if $k \geq 2$, if $P(k)$ is true, then $f_1 + f_2 + \cdots + f_{k-1} = f_{k+1} - 1$. Then

$$\begin{aligned}f_1 + f_2 + \cdots + f_{k-1}) + f_k &= (f_{k+1} - 1) + f_k \\ &= (f_{k+1} + f_k) - 1 \\ &= f_{k+2} - 1.\end{aligned}$$

This proves that if $P(k)$ is true, then $P(k+1)$ is true.

(f) Let $P(n)$ be, "$f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}$." For the inductive step, use

$$\begin{aligned}(f_1^2 + f_2^2 + \cdots + f_k^2) + f_{k+1}^2 &= f_k f_{k+1} + f_{k+1}^2 \\ f_1^2 + f_2^2 + \cdots + f_k^2 + f_{k+1}^2 &= f_{k+1}(f_k + f_{k+1}) \\ &= f_{k+1} f_{k+2}.\end{aligned}$$

6. For the inductive step, if $a_k = a \cdot r^{k-1}$, then

$$\begin{aligned}a_{k+1} &= r \cdot a_k \\ &= r(a \cdot r^{k-1}) \\ &= a \cdot r^k.\end{aligned}$$

8. For the inductive step, use the assumption that \(S_{k} = a(\dfrac{1 - r^{k}{1 - r})\) and the recursive definition to write $S_{k+1} = a + r \cdot S_k$.

9. (a) $a_2 = 7$, $a_3 = 12$, $a_4 = 17$, $a_5 = 22$, $a_6 = 27$.
(b) One possibility is: For each $n \in \mathbb{N}$, $a_n = 2 + 5(n-1)$.

12. (a) $a_2 = \sqrt{6}$, $a_3 = \sqrt{\sqrt{6}+5} \approx 2.729$, $a_4 \approx 2.780$, $a_5 \approx 2.789$, $a_6 \approx 2.791$
(b) Let $P(n)$ be, "$a_n < 3$." Since $a_1 = 1$, $P(1)$ is true. For $k \in \mathbb{N}$, if $P(k)$ is true, then $a_k < 3$. Now

$$a_{k+1} = \sqrt{5 + a_k}.$$

Since $a_k < 3$, this implies that $a_{k+1} < \sqrt{8}$ and hence, $a_{k+1} < 3$. This proves that if $P(k)$ is true, then $P(k+1)$ is true.

13. (a) $a_3 = 7$, $a_4 = 15$, $a_5 = 31$, $a_6 = 63$
(b) Think in terms of powers of 2.

14. (a) $a_3 = \dfrac{3}{2}$, $a_4 = \dfrac{7}{4}$, $a_5 = \dfrac{37}{24}$, $a_6 = \dfrac{451}{336}$

16. (b) $a_2 = 5$ $a_2 = 719$ $a_8 = 362879$
$a_3 = 23$ $a_2 = 5039$ $a_9 = 3628799$
$a_4 = 119$ $a_2 = 40319$ $a_{10} = 39916799$

18. (a) Let $P(n)$ be, "$L_n = 2f_{n+1} - f_n$." First, verify that $P(1)$ and $P(2)$ are true. Now let k be a natural number with $k \geq 2$ and assume that $P(1)$, $P(2)$, ..., $P(k)$ are all true. Since $P(k)$ and $P(k-1)$ are both assumed to be true, we can use them to help prove that $P(k+1)$ must then be true as follows:

$$\begin{array}{rcl} L_{k+1} & = & L_k + L_{k-1} \\ & = & (2f_{k+1} - f_k) + (2f_k - f_{k-1}) \\ & = & 2(f_{k+1} + f_k) - (f_k + f_{k-1} \\ & = & 2f_{k+2} - f_{k+1}. \end{array}$$

(b) Let $P(n)$ be, "$5f_n = L_{n-1} + L_{n+1}$." First, verify that $P(2)$ and $P(3)$ are true. Now let k be a natural number with $k \geq 3$ and assume that $P(2)$, $P(3)$, ..., $P(k)$ are all true. Since $P(k)$ and $P(k-1)$ are both assumed to be true, we can use them to help prove that $P(k+1)$ must then be true as follows:

$$\begin{array}{rcl} 5f_{k+1} & = & 5f_k + 5_{k-1} \\ & = & (L_{k-1} + L_{k+1}) + (L_{k-2} + Lk) \\ & = & (L_{k-1} + L_{k-2}) - (L_k + L_{k+1}) \\ & = & L_k + L_{k+2}. \end{array}.$$

Section 5.1

1. (a) $A = B$ (c) $C \neq D$ (e) $A \not\subseteq D$
(b) $A \subseteq B$ (d) $C \subseteq D$

2. In both cases, the two sets have preceisely the same elements.

3.

$$\begin{array}{ccccc} A & \subset, \subseteq, \neq & B\emptyset & \subset, \subseteq, \neq & A \\ 5 & \in & C\{5\} & \subset, \subseteq, \neq & C \\ |A| & = & |D|A & \in & \mathcal{P}(b) \end{array}$$

5. (a) The set $\{a, b\}$ is a not a subset of $\{a, c, d, e\}$ since $b \in \{a, b\}$ and $b \in \{a, c, d, e\}$.

7. (c) $(A \cup B)^c = \{2, 8, 10\}$ (h) $(A \cap C) \cup (B \cap C) = \{3, 6, 9\}$
(d) $A^c \cap B^c = \{2, 8, 10\}$ (n) $(A \cup B) - D = \{1, 3, 5, 7, 9\}$
(e) $(A \cup B) \cap C = \{3, 6, 9\}$

9. (b) There exists an $x \in U$ such that $x \in (P - Q)$ and $x \notin (R \cap S)$. This can be written as, There exists an $x \in U$ such that $x \in P$, $x \notin Q$, and $x \notin R$ or $x \notin S$.

10. (a) The given statement is a conditional statement. We can rewrite the subset relations in terms of conditional sentences: $A \subseteq B$ means, "For all $x \in U$, if $x \in A$, then $x \in B$," and $B^c \subseteq A^c$ means, "For all $x \in U$, if $x \in B^c$, then $x \in A^c$."

Section 5.2

1. (a) The set A is a subset of B. A proof is required. The idea is that if $x \in A$, then $-2 < x < 2$. Since $x < 2$, we conclude that $x \in B$.
(b) The set B is not a subset of A. Give an example of a real number that is in B but not in A.

3. (b) $A \subseteq B$ $B \nsubseteq A$

7. (a) Start by letting x be an element of $A \cap B$.
(b) Start by letting x be an element of A.
(e) By Theorem 5.1, $\emptyset \subseteq A \cap \emptyset$. By Part (a), $A \cap \emptyset \subseteq \emptyset$. Therefore, $A \cap \emptyset = \emptyset$.

12. (a) Let $x \in A \cap C$. Then $x \in A$ and $x \in C$. Since we are assuming that $A \subseteq B$, we see that $x \in B$ and $x \in C$. This proves that $A \cap C \subseteq B \cap C$.

15. (a) "If $A \subseteq B$, then $A \cap B^c = \emptyset$" is Proposition 5.14. To prove the other conditional statement, start with, "Let $x \in A$." Then use the assumption that $A \cap B^c = \emptyset$ to prove that x must be in B.
(b) To prove "If $AsubseteqB$, then $A \cup B = B$," first note that if $x \in B$, then $x \in A \cup B$ and, hence, $B \subseteq A \cup B$. Now let $x \in A \cup B$ and note that since $A \subseteq B$, if $x \in A$, then $x \in B$. Use this to argue that under the assumption that $A \subseteq B$, $A \cup B \subseteq B$.

Tp prove "If $A \cup B = B$, then $A \subseteq B$," start with, Let $x \in A$ and use this asusmption to prove that x must be an element of B.

Section 5.3

1. (a) Let $x \in (A^c)^c$. Then $x \notin A^c$, which means $x \in A$. Hence, $(A^c)^c \subseteq A$. Now prove that $A \subseteq (A^c)^c$.
(c) Let $x \in U$. Then $x \notin \emptyset$ and so $x \in \emptyset^c$. Therefore, $U \subseteq \emptyset^c$. Also, since every set we deal with is a subset of the universal set, $\emptyset^c \subseteq U$.

2. We will first prove that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. So we will use two cases: (1) $x \in B$; (2) $x \in C$. In Case (1), $x \in A \cap B$ and, hence $x \in (A \cap B) \cup (A \cap C)$. In Case (2), $x \in A \cap C$ and, hence, $x \in (A \cap B) \cup (A \cap C)$. This proves that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Now prove that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

4. (a) $A - (B \cup C) = (A - B) \cap (A - C)$.
(c) Using the algebra of sets, we obtain

$$\begin{aligned} (A - B) \cap (A - C) &= (A \cap B^c) \cap (A \cap C^c) \\ &= (A \cap A) \cap (B^c \cap C^c) \\ &= A \cap (B \cup C)^c \\ &= A - (B \cup C). \end{aligned}$$

9. (a) Use a proof by contradiction. Assume the sets are not disjoint and let $x \in A \cap (B - A)$. Then $x \in A$ and $x \in B - A$, which implies that $x \notin A$.

Section 5.4

1, (a) $A \times B = \{(1, a), (1, b), (1, c), (1, d), (2, a), (2, b), (2, c), (2, d)\}$
(b) $B \times A = \{(a, 1), (b, 1), (c, 1), (d, 1), (a, 2), (b, 2), (c, 2), (d, 2)\}$
(c) $A \times (B \cap C) = \{(1, a), (1, b), (2, a), (2, b)\}$

3. Start of proof that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$:
Let $u \in A \times (B \cap C)$. Then there exists $x \in A$ and there exists $y \in B \cap C$ such that $u = (x, y)$. Since $y \in B \cap C$, we know that $y \in B$ and $y \in C$. So we have

$$u = (x, y), \text{ where } x \in A \text{ and } y \in B. \text{ This means that } u \in A \times B.$$
$$u = (x, y), \text{ where } x \in A \text{ and } y \in C. \text{ This means that } u \in A \times C.$$

4. Start of proof that $(A \cup B) \times C \subseteq (A \times C) \cup (B \times C)$:

let $u \in (A \cup B) \times C$. Then there exists $x \in A \cup B$ and there exists $y \in C$ such that $u = (x, y)$. Since $x \in A \cup B$, we know that $x \in A$ or $x \in B$.

Section 5.5

1. (a) {3, 4}
(d) {3, 4, 5, 6, 7, 8, 9, 10}

2. (a) {5, 6, 7, ...}
(c) $\emptyset$
(d) {1, 2, 3, 4}
(f) $\emptyset$

3. (a) $\{x \in \mathbb{R} \mid -100 \leq x \leq 100\}$
(b) $\{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$

4. (a) We let $\beta \in \Lambda$ and let $x \in A_\beta$. Then $x \in A_\alpha$, for at lest one $\alpha \in \Lambda$ and, hence, $x \in \bigcup_{\alpha \in \Lambda} A_\alpha$. This proves that $A_\beta \subseteq \bigcup_{\alpha \in \Lambda} A_\alpha$.

5. (a) We first let $x \in B \cap (\bigcup_{\alpha \in \Lambda} A_\alpha)$. Then $x \in B$ and $x \in \bigcup_{\alpha \in \Lambda} A_\alpha$. This means that there exists an $\alpha \in \Lambda$ such that $x \in A_\alpha$. Hence, $x \in B \cap A_\alpha$, which implies that $x \in \bigcup_{\alpha \in \Lambda}(B \cap A_\alpha)$. This prove that $B \cap (\bigcup_{\alpha \in \Lambda} A_\alpha) \subseteq \bigcup_{\alpha \in \Lambda}(B \cap A_\alpha)$, and we still need to prove that $\bigcup_{\alpha \in \Lambda}(B \cap A_\alpha) \subseteq B \cap (\bigcup_{\alpha \in \Lambda} A_\alpha)$.

8. (a) Let $x \in B$. For each $\alpha \in \Lambda$, $B \subseteq A_\alpha$ and, hence, $x \in A_\alpha$. This means that for each $\alpha \in \Lambda$, $x \in A_\alpha$ and, hence, $x \in \bigcap_{\alpha \in \Lambda} A_\alpha$. Therefore, $B \subseteq \bigcap_{\alpha \in \Lambda} A_\alpha$

12. (a) We first rewrite the set difference and then use a distributive law.

$$\begin{aligned}
(\textstyle\bigcup_{\alpha \in \Lambda} A_\alpha) - B &= (\textstyle\bigcup_{\alpha \in \Lambda} A_\alpha) \cap B^c \\
&= \textstyle\bigcup_{\alpha \in \Lambda}(A_\alpha \cap B^c) \\
&= \textstyle\bigcup_{\alpha \in \Lambda}(A_\alpha - B)
\end{aligned}$$

Section 6.1

1. (a) $f(-3) = 15$, $f(-1) = 3$, $f(1) = -1$, $f(3) = 3$.

(b) The set of preimages of 0 is {0, 2}. The set of preimages of 4 is $\{\dfrac{2-\sqrt{20}}{2}, \dfrac{2+\sqrt{20}}{2}\}$. (Use the quadratic formula.)
(d) range$(f) = \{y \in \mathbb{R} \mid y \geq -1\}$.

4. (b) The set of preimages of 5 is {2}. There set of preimages of 4 is $\emptyset$.
(c) The range of the function f is the set of all odd integers.
(d) The graph of the function f consists of an infinite set of discrete points.

5. (b) dom$(F) = \{x \in \mathbb{R} \mid x > \dfrac{1}{2}\}$, range$(F) = \mathbb{R}$
(d) dom$(g) = \{x \in \mathbb{R} \mid x \neq 2 \text{ and } x \neq -2\}$,
range$(g) = \{y \in \mathbb{R} \mid y > 0\} \cup \{y \in \mathbb{R} \mid y \leq -1\}$

6. (a) $d(1) = 1$, $d(2) = 2$, $d(3) = 2$, $d(4) = 3$, $d(8) = 4$, $d(9) = 3$
(c) The only natural numbers n such that $d(n) = 2$ are the prime numbers. The set of preimages of the natural number 2 is the set of prime numbers.
(e) $d(2^0) = 1$, $d(2^1) = 2$, $d(2^2) = 3$, $d(2^3) = 4$
(f) The divisors of 2^n are 2^0, 2^1, 2^2, ..., 2^{n-1}, 2^n.

7. (a) The domain of S is $\mathbb{N}$. The power set of $\mathbb{N}$, $[\mathcal{P}(\mathbb{N})]$ can be the codomain. The rule for determining outputs is that for each $n \in \mathbb{N}$, $S(n)$ is the set of all distinct natural number factors of n.
(b) For example, $S(8) = \{1, 2, 4, 8\}$, $S(15) = \{1, 3, 5, 15\}$.
(c) For example, $S(2) = \{1, 2\}$, $S(3) = \{1, 3\}$, $S(31) = \{1, 31\}$.

Section 6.2

1. (a) $f(0) = 4$, $f(1) = 0$, $f(2) = 3$, $f(3) = 3$, $f(4) = 0$
(b) $g(0) = 4$, $g(1) = 0$, $g(2) = 3$, $g(3) = 3$, $g(4) = 0$
(c) The two functions are equal.

2. (c) The two functions are not equal. For example, $f(1) = 5$ and $g(1) = 4$.

4. (a) $\langle a_n \rangle$, where $a_n = \cos(n\pi)$ for each $n \in \mathbb{N}$. The domain is $\mathbb{N}$, and {-1, 1} can be the codomain. This sequence is equal to the sequence in Part (c).

5. (a) $p_1(1, x) = 1$, $p_1(1, y) = 1$, $p_1(1, z) = 1$, $p_1(2, x) = 2$, $p_1(2, y) = 2$, $p_1(2, z) = 2$
(c) range$(p_1) = A$, range$(p_2) = B$

6. Start of the inductive step: Let $P(n)$ be "A convex polygon with n sides has $\dfrac{n(n-3)}{2}$ diagonals." Let $k \in D$ and assume that $P(k)$ is true, that is, a convex polygon with k sides has $\dfrac{k(k-3)}{2}$ diagonals. Now let Q be convex polygon with $(k+1)$ sides. Let v be one of the $(k+1)$ vertices of Q and let u and w be the two vertices adjacent to v. By drawing the line segment from u to w and omitting the vertex v, we form a convex polygon with k sides. Now complete the inductive step.

7. (a) $f(-3,4) = 9$, $f(-2,-7) = -23$
(b) $\{(m,n) \in \mathbb{Z} \times \mathbb{Z} \mid m = 4 - 3n\}$

9. (a) det$\begin{bmatrix} 3 & 5 \\ 4 & 1 \end{bmatrix}$ = -17, det$\begin{bmatrix} 1 & 0 \\ 0 & 7 \end{bmatrix}$ = 7, and det$\begin{bmatrix} 3 & -2 \\ 5 & 0 \end{bmatrix}$ = 10.

Section 6.3

2. (a) The function f is not an injection and is not a surjection.
(c) The function F is an injection and is a surjection.

3. (a) The function f is an injection and is not a surjection.
(b) The function F is an injection and is a surjection.

4. (a) Let $F : \mathbb{R} \to \mathbb{R}$ be defined by $F(x) = 5x + 3$ for all $x \in \mathbb{R}$. Let $x_1, x_2 \in \mathbb{R}$ and assume that $F(x_1) = F(x_2)$. Then $5x_1 + 3 = 5x_2 + 3$. Show that this implies that $x_1 = x_2$ and, hence, F is an injection.
Now let $y \in \mathbb{R}$. Then $\dfrac{y-3}{5} \in \mathbb{R}$. Prove that $F(\dfrac{y-3}{5}) = y$. Thus, F is a sjection and hence F is a bijection.
(b) Notice that for each $x \in \mathbb{Z}$, $G(x) \equiv 3$ (mod 5). Now explain why G is not a surjection.

7. The birthday function is not an injection since there are two different people with the same birthday. The birthday function is a surjection since for each day of the year, there is a person that was born on that day.

9. (a) The function f is an injection and a surjection.
(b) The function g is an injection and is not a surjection.

Section 6.4

3. (a) $F(x) = (g \circ f)(x)$, $f(x) = e^x$, $g(x) = \cos x$
(b) $G(x) = (g \circ f)(x)$, $f(x) = \cos x$, $g(x) = e^x$

4. (a) For each $x \in A$. $(f \circ I_A)(x) = f(I_A(x)) = f(x)$. Therefore, $f \circ I_A = f$.

5. (a) $[(h \circ g) \circ f](x) = \sqrt[3]{\sin(x^2)}$; $[h \circ (g \circ f)](x)\sqrt[3]{\sin(x^2)}$

6. Start of a proof: Let A, B, and C be nonempty sets and let $f : A \to B$ and $g : B \to C$. Assume that f and g are both injections. Let $x, y \in A$ and assume that $(g \circ f)(x) = (g \circ f)(y)$.

7. (a) $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x$, $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^2$. The function f is a surjection, but $g \circ f$ is not a surjection.
(f) By Part (1) of Theorem 6.21, this is not possible since if $g \circ f$ is an injection, then f is an injection.

Section 6.5

2. (b) $f^{-1} = \{(c,a), (b,b), (d,c), (a,d)\}$
(d) $(f^{-1} \circ f)(x) = x = (f \circ f^{-1})(x)$. This illustrates Corollary 6.28.

4. Using the notation from Corollary 6.28, if $y = f(x)$ and $x = f^{-1}(y)$, then

$$\begin{array}{rcl} (f \circ f^{-1}(y) & = & f(f^{-1}(y)) \\ & = & f(x) \\ & = & y \end{array}$$

6. (a) Let $x, y \in A$ and assume that $f(x) = f(y)$. Apply g to both sides of this equation to prove that $(g \circ f)(x) = (g \circ f)(y)$. Since $g \circ f = I_A$, this impliies that $x = y$ and hence that f is an injection.
(b) Start by assuming that $f \circ g = I_B$, and then let $y \in B$. You need to prove there exists an $x \in A$ such that $f(x) = y$.
(d) $g : \mathbb{R}^+ \to \mathbb{R}$ by $g(y) = \dfrac{1}{2}(\text{In} y + 1)$

7. The inverse of f is not a function and the inverse of g is a function.

Section 6.6

1. (a) There exists an $x \in A \cap B$ such that $f(x) = y$.
(d) There exists an $a \in A$ such that $f(a) = y$ or there exists a $b \in B$ such that $f(b) = y$.
(f) $f(x) \in C \cup D$
(h) $f(x) \in C$ or $f(x) \in D$.

2. (b) $f^{-1}(f(A)) = [2, 5]$.
(e) $f(A \cap B) = [-5, -3]$
(d) $f(f^{-1}(C)) = [-2, 3]$
(f) $f(A) \cap f(B) = [-5, -3]$

3. (a) $g(A \times A) = \{6, 12, 18, 24, 36, 54, 72, 108, 216\}$
(b) $g^{-1}(C) = \{(1, 1), (2, 1), (1, 2)\}$

4. (a) range$(F) = F(S) = \{1, 4, 9, 16\}$

5. To prove $f(A \cup B) \subseteq f(A) \cup f(B)$, start by letting $y \in f(A \cup B)$. This means that there exists an x in $A \cup B$ such that $f(x) = y$. How do you prove that $y \in f(A) \cup f(B)$?

6. To prove that $f^{-1}(C \cap D) \subseteq f^{-1}(C) \cap f^{-1}(D)$, let $x \in f^{-1}(C \cap D)$. Then $f(x) \in C \cap D$. How do you prove that $x \in f^{-1}(C) \cap f^{-1}(D)$?

9. Statement (a) is true and Statement (b) is false.

Section 7.1

1. (a) The set $A \times B$ contains nine ordered pairs. The set $A \times B$ is a relation from A to B since $A \times B$ is a subset of $A \times B$.
(b) The set R is a relation from A to B since $R \subseteq A \times B$.
(c) dom$(R) = A$, range$(R) = \{p, q\}$
(d) $R^{-1} = \{(p, a), (q, b), (p, c), (q, a)\}$

2. Only the statement in Part (b) is true.

3. (a) The domain of D consists of the female citizens of the United States whose mother is a female citizen of the United States.
(b) The range of D consists of those female citizens of the United States who have a daughter that is a female citizen of the United States.

4. (a) $(S, T) \in R$ means that $S \subseteq T$.
(b) The domain of the subset relation is $\mathcal{P}(U)$.
(c) The range of the subsetr elation is $\mathcal{P}(U)$.
(d) $R^{-1} = \{(T, S) \in \mathcal{P}(U) \times \mathcal{P}(U) \mid S \subseteq T\}$.
(e) The relation R is not a function from $\mathcal{P}(U)$ to $\mathcal{P}(U)$ since any proper subset of U is a subset of more than one subset of U.

6. (a) $\{x \in \mathbb{R} \mid (x, 6) \in S\} = \{-8, 8\}$
$\{x \in \mathbb{R} \mid (x, 9) \in S\} = \{-\sqrt{19}, \sqrt{19}\}$
(b) The domain and range of S is the closed interval [-10, 10].
(d) The relation S is not a function from $\mathbb{R}$ to $\mathbb{R}$.

9. (a) $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid |a - b| \leq 2\}$
(b) dom$(R) = \mathbb{Z}$ and range$(R) = \mathbb{Z}$

Section 7.2

1. The relation R is not reflexive on A and is not symmetric. However, it is transitive since the conditional statement "For all $x, y, z \in A$, if $x\ R\ y$ and $y\ R\ z$, then $x\ R\ z$" is a true conditional statement.

4. The relation R is not reflexive on A, is symmetric, and is not transitive.

6. (a) The relation $\sim$ is an equivalence relation.
(b) $C = \{-5, 5\}$

10. The relation $\sim$ is an equivalence relation and the relation $\approx$ is not an equivalence relation.

15. (c) The set C is a circle of radius 5 with center at the origin.

Section 7.3

1. $[a] = [b] = \{a, b\}$; $[c] = \{c\}$; $[d] = [e] = \{d, e\}$

2. $[a] = [b] = [d] = \{a, b, d\}$; $[c] = \{c\}$; $[e] = [f] = \{e, f\}$

3. The equivalence classes are {0, 1, 2, ..., 9}, {10, 11, 12, ..., 99}, {100, 101, 102, ..., 999}, {1000}.

4. The congruence classes for the relation of congruence modulo 5 on the set of integers are

$[0] = \{5n \mid n \in \mathbb{Z}$ $[3] = \{5n + 3 \mid n \in \mathbb{Z}$
$[1] = \{5n + 1 \mid n \in \mathbb{Z}$
$[2] = \{5n + 2 \mid n \in \mathbb{Z}$ $[4] = \{5n + 4 \mid n \in \mathbb{Z}$

5. (a) The distinct equivalence classes are {0, 3, 6}, {1, 8}, {2, 7}, and {4, 5}.

6. (a) Let $x \in [\frac{5}{7}]$. Then $x - \frac{5}{7} \in \mathbb{Z}$, which means that there is an integer m such that $x - \frac{5}{7} = m$, or $x = \frac{5}{7} + m$. This proves that $x \in \{m + \frac{5}{7} \mid m \in \mathbb{Z}\}$ and, hence, that $[\frac{5}{7}] \subseteq \{m + \frac{5}{7} \mid m \in \mathbb{Z}\}$. We still need to prove that $\{m + \frac{5}{7} \mid m \in \mathbb{Z}\} \subseteq [\frac{5}{7}]$

9. (a) To prove the relation is symmetric, note that if $(a, b) \approx (c, d)$, then $ad = bc$. This implies that $cb = da$ and, hence, $(c, d) \approx (a, b)$
(c) $3a = 2b$

Section 7.4

1. (a)

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\odot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[0]	[1]	[2]	[3]	[4]	[5]

(b)

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

2. (a) $[x] = [1]$ or $[x] = [3]$
(e) $[x] = [2]$ or $[x] = [3]$
(g) The equation has no solution.

3. The statement in (a) is false. The statement in (b) is true.

5. (a) The proof consists of the following computations:

$$\begin{array}{ll} [1]^1 = [1] & [3]^1 = [9] = [4] \\ [2]^1 = [4] & [4]^1 = [16] = [1]. \end{array}$$

17. (a) Prove the contrapostive by calculating $[a]^2 + [b]^2$ for all nonzero $[a]$ and $[b]$ in $\mathbb{Z}_3$.

Section 8.1

1. (a) gcd(21, 28) = 7
(b) gcd(-21, 28) = 7
(c) gcd(58, 63) = 1
(d) gcd(0, 12) = 12

2. (a) **Hint**: Prove that $k \mid [(a+1)-a]$.

4. (a) $|b|$ is the largest natural number that divides 0 and b.
(b) The integers b and $-b$ have the same divisors. Therefore, $\gcd(a,-b) = \gcd(a,b)$.

5. (a) gcd(36, 60) = 12 $12 = 36 \cdot 2 + 60 \cdot (-1)$
(a) gcd(901, 935) = 17 $17 = 901 \cdot 27 + 935 \cdot (-26)$
(a) gcd(901, -935) = 17 $17 = 901 \cdot 27 + (-935) \cdot (26)$

7. (a) $11 \cdot (-3) + 17 \cdot 2 = 1$
(b) $\frac{m}{11} + \frac{n}{17} = \frac{17m+11n}{187}$

Section 8.2

1. The only natural number divisors of a prime number p are 1 and p.

2. Use cases: (1) p divides a; (2) p does not divide a. In this case, use the fact that gcd(a, p) = 1 to write the number 1 as a linear combination of a and p.

3. A hint for the inductive step: Write $p \mid (a_1 a_2 \cdots a_m) a_{m+1}$. Then look at two cases: (1) $p \mid a_{m+1}$; (2) p does not divide a_{m+1}.

4. (a) gcd(a, b) = 1. Why?
(b) gcd(a, b) = 1 or gcd(a, b) = 1=2. Why?

7. (a) gcd(16, 28) = 4. Also, $\frac{16}{4} = 4$, $\frac{28}{4} = 7$, and gcd(4, 7) = 1.

9. Part (b) of Exercise (8) can be helpful.

11. The statement is true. Start of a proof: If gcd(a, b) = 1 and $c \mid (a+b)$, then there exist integers x and y such that $ax + by = 1$ and there exists an integer m such that $a + b = cm$.

Section 8.3

3. (a) $x = -3 + 14k, y = 2 - 9k$
(b) $x = -1 + 11k, y = 1 + 9k$
(c) No solution
(d) $x = 2 + 3k, y = -2 - 4k$

4. There are several possible solutions to this problem, each of which can be generated from the solutions of the Diophantine equation $27x + 50y = 25$.

5. This problem can be solved by finding all solutions of a linear Diophantine equation in x and y, where both x and y are positive. The minimum number of people attending the banquet is 66.

6. (a) $y = 12 + 16k$, $x_3 = -1 - 3k$
(c) $x_1 = y + 3n$, $x_2 = -y + 4n$

Section 9.1

2. Use $f : A \times \{x\} \to A$ by $f(a,x) = a$, for all $(a,x) \in A \times \{x\}$.

4. Notice that $A = (A - \{x\}) \cup \{x\}$. Use Theorem 9.6 to conclude that $A - \{x\}$ is finte. Then use Lemma 9.4.

5. (a) Since $A \cap B \subseteq A$, if A is finite, then Theorem 9.6 implies that $A \cap B$ is finte.

7. (a) Remember that two ordered pairs are equal if and only if their corresponding coordinates are equal. So if $h(a_1,c_1) = h(a_2,c_2)$, then $(f(a_1), g(c_1)) = (f(a_2), g(c_2))$. We can then conclude that $f(a_1) = f(a_2)$ and $g(c_1) = g(c_2)$.

8. (a) If we define the function f by $f(1) = a$, $f(2) = b$, $f(3) = c$, $f(4) = a$, and $f(5) = b$, then we can use $g(a) = 1$, $g(b) = 1$, and $g(3)$ $= c$. The function g is an injection.

Section 9.2

1. All except Part (d) are true.

2. (e) Either define an appropriate bijection or use Corollary 9.20 to conclude that $\mathbb{N} - \{4, 5, 6\}$ is countable. Prove that $\mathbb{N} - \{4, 5, 6\}$ cannot be finite.
(f) $\{m \in \mathbb{Z} \mid m \equiv 2 \pmod 3\} = \{3k + 2 \mid k \in \mathbb{Z}\}$

5. For each $n \in \mathbb{N}$, let $P(n)$ be "If card(B) = n, then $A \cup B$ is a countably infinte set."

Note that if card$(B) = k + 1$ and $x \in B$, then card$(B - \{x\}) = k$. Apply the inductive assumption to $B - \{x\}$.

6. Notice that if $h(n) = h(m)$, then since A and B are disjoint, either $h(n)$ and $h(m)$ are both in A or are both in B.

Also, if $y \in A \cup B$, then there are only two cases to consider: $y \in A$ or $y \in B$.

8. Since $A - B \subseteq A$, the set $A - B$ is countable. Now assume $A - B$ is finte and show that this leads to a contradiction.

Section 9.3

1. (a) $f : (0, \infty) \to \mathbb{R}$ by $f(x) = \text{In}x$ for all $x \in (0, \infty)$
(b) $g : (0, \infty) \to (a, \infty)$ by $g(x) = x + a$ for all $x \in (0, \infty)$. The function g is a bijection and so $(0, \infty) \approx (a, \infty)$. Then use Part (a).

2. Show that the assumption that the set of irrational numbers is countable leads to a contradiction.

3. Use Corollary 9.20.

Appendix D: List of Symbols

Symbol	**Meaning**
$\to$	Conditional statement
$\mathbb{R}$	set of real numbers
$\mathbb{Q}$	set of rational numbers
$\mathbb{Z}$	set of integers
$\mathbb{N}$	set of natural numbers
$y \in A$	y is an element of A
$z \notin A$	z is not an element of A
$\{ \mid \}$	set builder notation
$\forall$	universal quantifier
$\exists$	existential quantifier
$\emptyset$	the empty set
$\wedge$	conjunction
vee	disjunction
$\neg$	negation
$\leftrightarrow$	biconditional statement
$\equiv$	logically equivalent
$m \mid n$	m divides n
$a \equiv b \pmod{n}$	a is congruent to b modulo n
$\lvert x \rvert$	the absolute value of x
$A = B$	A equals B (set equality)
$A \subseteq B$	A is a subset of B
$A \nsubseteq B$	A is not a subset of B
$A \subset B$	A is a proper subset of B
$\mathcal{P}(A)$	power set of A
$\lvert A \rvert$	cardinality of a finite set A
$A \cap B$	intersection of A and B
A^c	complement of A
$A - B$	set difference of A and B
$A \times B$	Cartesian product of A and B
(a, b)	ordered pair
$\mathbb{R} \times \mathbb{R}$	Cartesian plane
$\mathbb{R}^2$	Cartesian plane
\(\bigcup_{X \in \mathcal{C}} X\)	union of a family of sets

\(\bigcap_{X \in \mathcal{C}} X\)	intersection of a finite family of sets
$\bigcup_{j=1}^{n} A_j$	union of a finite family of sets
$\bigcap_{j=1}^{n} A_j$	intersection of a finite family of sets
$\bigcup_{j=1}^{\infty} B_j$	union of an infinite family of sets
$\bigcap_{j=1}^{\infty} B_j$	intersection of a infinite family of sets
$\{A_\alpha \mid \alpha \in \Lambda\}$	indexed family of sets
$\bigcup_{\alpha \in \Lambda} A_\alpha$	union of an indexed family of sets
$\bigcap_{\alpha \in \Lambda} A_\alpha$	intersection of an indexed family of sets
$n!$	n factorial
$f_1, f_2, f_3, \ldots$	Fibonacci numbers
$s(n)$	sum of the divisors of n
$f : A \to B$	function from A to B
dom(f)	domain of the function f
codom(f)	codmain of the function f
$f(x)$	inage of x under f
range(f)	range of the function f
$d(n)$	number of divisors of n
I_A	identity function on the set A
p_1, p_2	projection functions
det(A)	determinant of A
A^T	transpose of A
det: $M_{2,2} \to \mathbb{R}$	determinant function
$g \circ f : A \to C$	composition of function f and g
f^{-1}	the inverse of the function f
Sin	the restricted sine function
Sin^{-1}	the inverse sine function
dom(R)	domain of the relation R
range(R)	range of the relation R
$x\ R\ y$	x is related to y
$x \not R\ y$	x is not related to y
$x \sim y$	x is related to y
$x \nsim y$	x is not related to y
R^{-1}	the inverse of the relation R
$[a]$	equivalence class of a
$[a]$	congruence class of a

$\mathbb{Z}_n$	the integers modulo n
$[a] \oplus [c]$	addition in $\mathbb{Z}_n$
$[a] \odot [c]$	multiplication in $\mathbb{Z}_n$
gcd(a, b)	greatest common divisor of a and b
$f(A)$	image of A under the function f
$f^{-1}(C)$	pre-image of C under the funtion f
$A \approx B$	A is equivalent to B A and B have the same cardinality
$\mathbb{N}_k$	$\mathbb{N}_k = \{1, 2, ..., k\}$
card$(A) = k$	cardinality of A is k
$aleph_0$	cardinality of $\mathbb{N}$
c	cardinal number of the continuum

Detailed Licensing

Overview

Title: Mathematical Reasoning - Writing and Proof (Sundstrom)

Webpages: 68

Applicable Restrictions: Noncommercial

All licenses found:

- CC BY-NC-SA 3.0: 86.8% (59 pages)
- Undeclared: 13.2% (9 pages)

By Page

- Mathematical Reasoning - Writing and Proof (Sundstrom) - *CC BY-NC-SA 3.0*
    - Front Matter - *Undeclared*
        - TitlePage - *Undeclared*
        - InfoPage - *Undeclared*
        - Table of Contents - *Undeclared*
        - Licensing - *Undeclared*
    - 1: Introduction to Writing Proofs in Mathematics - *CC BY-NC-SA 3.0*
        - 1.1: Statements and Conditional Statements - *CC BY-NC-SA 3.0*
        - 1.2: Constructing Direct Proofs - *CC BY-NC-SA 3.0*
        - 1.S: Introduction to Writing Proofs in Mathematics (Summary) - *CC BY-NC-SA 3.0*
    - 2: Logical Reasoning - *CC BY-NC-SA 3.0*
        - 2.1: Statements and Logical Operators - *CC BY-NC-SA 3.0*
        - 2.2: Logically Equivalent Statements - *CC BY-NC-SA 3.0*
        - 2.3: Open Sentences and Sets - *CC BY-NC-SA 3.0*
        - 2.4: Quantifiers and Negations - *CC BY-NC-SA 3.0*
        - 2.S: Logical Reasoning (Summary) - *CC BY-NC-SA 3.0*
    - 3: Constructing and Writing Proofs in Mathematics - *CC BY-NC-SA 3.0*
        - 3.1: Direct Proofs - *CC BY-NC-SA 3.0*
        - 3.2: More Methods of Proof - *CC BY-NC-SA 3.0*
        - 3.3: Proof by Contradiction - *CC BY-NC-SA 3.0*
        - 3.4: Using Cases in Proofs - *CC BY-NC-SA 3.0*
        - 3.5: The Division Algorithm and Congruence - *CC BY-NC-SA 3.0*
        - 3.6: Review of Proof Methods - *CC BY-NC-SA 3.0*
        - 3.S: Constructing and Writing Proofs in Mathematics (Summary) - *CC BY-NC-SA 3.0*
    - 4: Mathematical Induction - *CC BY-NC-SA 3.0*
        - 4.1: The Principle of Mathematical Induction - *CC BY-NC-SA 3.0*
        - 4.2: Other Forms of Mathematical Induction - *CC BY-NC-SA 3.0*
        - 4.3: Induction and Recursion - *CC BY-NC-SA 3.0*
        - 4.S: Mathematical Induction (Summary) - *CC BY-NC-SA 3.0*
    - 5: Set Theory - *CC BY-NC-SA 3.0*
        - 5.1: Sets and Operations on Sets - *CC BY-NC-SA 3.0*
        - 5.2: Proving Set Relationships - *CC BY-NC-SA 3.0*
        - 5.3: Properties of Set Operations - *CC BY-NC-SA 3.0*
        - 5.4: Cartesian Products - *CC BY-NC-SA 3.0*
        - 5.5: Indexed Families of Sets - *CC BY-NC-SA 3.0*
        - 5.S: Set Theory (Summary) - *CC BY-NC-SA 3.0*
    - 6: Functions - *CC BY-NC-SA 3.0*
        - 6.1: Introduction to Functions - *CC BY-NC-SA 3.0*
        - 6.2: More about Functions - *CC BY-NC-SA 3.0*
        - 6.3: Injections, Surjections, and Bijections - *CC BY-NC-SA 3.0*
        - 6.4: Composition of Functions - *CC BY-NC-SA 3.0*
        - 6.5: Inverse Functions - *CC BY-NC-SA 3.0*
        - 6.6: Functions Acting on Sets - *CC BY-NC-SA 3.0*
        - 6.S: Functions (Summary) - *CC BY-NC-SA 3.0*
    - 7: Equivalence Relations - *CC BY-NC-SA 3.0*
        - 7.1: Relations - *CC BY-NC-SA 3.0*
        - 7.2: Equivalence Relations - *CC BY-NC-SA 3.0*
        - 7.3: Equivalence Classes - *CC BY-NC-SA 3.0*
        - 7.4: Modular Arithmetic - *CC BY-NC-SA 3.0*
        - 7.S: Equivalence Relations (Summary) - *CC BY-NC-SA 3.0*
    - 8: Topics in Number Theory - *CC BY-NC-SA 3.0*
        - 8.1: The Greatest Common Divisor - *CC BY-NC-SA 3.0*
        - 8.2: Prime Numbers and Prime Factorizations - *CC BY-NC-SA 3.0*
        - 8.3: Linear Diophantine Equations - *CC BY-NC-SA 3.0*

  - 8.S: Topics in Number Theory (Summary) - *CC BY-NC-SA 3.0*
- 9: Finite and Infinite Sets - *CC BY-NC-SA 3.0*
  - 9.1: Finite Sets - *CC BY-NC-SA 3.0*
  - 9.2: Countable Sets - *CC BY-NC-SA 3.0*
  - 9.3: Uncountable Sets - *CC BY-NC-SA 3.0*
  - 9.S: Finite and Infinite Sets (Summary) - *CC BY-NC-SA 3.0*
- Back Matter - *Undeclared*
  - Index - *Undeclared*
  - Glossary - *Undeclared*
  - Appendix A: Guidelines for Writing Mathematical Proofs - *CC BY-NC-SA 3.0*
  - Appendix B: Answers for the Progress Checks - *CC BY-NC-SA 3.0*
  - Appendix C: Answers and Hints for Selected Exercises - *CC BY-NC-SA 3.0*
  - Appendix D: List of Symbols - *CC BY-NC-SA 3.0*
  - Detailed Licensing - *Undeclared*